

Net Guardian 832A

USER MANUAL



Visit our website at www.dpstelecom.com for the latest PDF manual and FAQs.

July 19, 2001

UM00C.30240
Used in conjunction with UM006.12201

Firmware: 2.1-2.5

Revision History

3/1/01 - UM00C.30221	User Manual released. Supports firmware version 2.0
7/18/01 - UM00C.30240	Split Web Server into separate user manual (UM006.12201) Revised to support firmware versions 2.1 to 2.5.

The material in this manual is for information purposes and is subject to change without notice. DPS Telecom shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance or use of this manual.

This document contains proprietary information which is protected by copyright. All rights are reserved. No part of this document may be photocopied without prior written consent of DPS Telecom.

© Copyright 2001, DPS Telecom

Table of Contents

Visit our website at www.dpstelecom.com for the latest PDF manual and Net Guardian FAQs.

Overview Chapter 1	1
1.1 Summary of Features	1
1.2 Introduction	2
Hardware Chapter 2	3
2.1 Shipping List	3
2.2 Specifications	4
2.3 Hardware Installation	5
2.3.1 Site Preparation	5
2.3.2 Installation Steps Overview	5
2.3.3 Mounting Instructions	6
2.3.4 Power Connection	7
2.3.5 Communication Lines	7
2.3.5.1 LAN Connection	7
2.3.5.2 Phone Line Connection	7
2.3.6 Alarm and Relay connections	8
2.3.6.1 Discrete Alarms	8
2.3.6.2 Control Points (Relays)	8
2.3.6.3 Analog Alarm Channels	8
2.3.6.4 66 Block	9
2.3.6.5 Net Guardian 832A Back Panel	11
2.3.7 Proxy Connections (Reach through Ports)	12
2.3.8 PCB Settings	13
2.4 Net Guardian Accessory Installation	15
2.4.1 Hinged wire wrap back panel	15
2.4.1.1 Plexi-glass wire-wrap cover	15
Software Provisioning Chapter 3	16
3.1 Connecting to the Net Guardian	16
3.1.1 Web Server	16
3.1.2 Local Connection	16
3.1.3 Remote Connection (Dial-up)	16
3.1.4 LAN Connection	16
3.2 LAN/WAN setup	17
3.3 Entering System Settings	18
3.4 Changing the Logon Password	19
3.5 Configuring Port Parameters	20
3.5.1 Setting Ethernet Port Values	20
3.5.1.1 Using the Base URL field	21
3.5.2 MIB Installation	21
3.5.3 Setting Modem Port Values	21
3.5.4 Setting Craft Port Values	22
3.5.5 Setting the Data Port Values	23
3.6 Setting Up Notification Methods from the Pagers Screen	24
3.6.1 Alpha numeric pager setup	25
3.6.2 Numeric pager setup	25
3.6.3 Text paging setup	25
3.6.4 T/MonXM paging setup	25
3.6.5 E-mail paging setup	25

3.6.6 SNMP paging setup	26
3.6.7 TCP paging setup	26
3.7 Configuring Base Discrete Alarms	27
3.8 Configuring the Controls (Relays)	28
3.8.1 Echoing alarm points to relays.	28
3.9 Setting the Analog Parameters	29
3.10 Configuring Ping Targets	31
3.11 Setting System Timers	32
3.12 Setting the System Date and Time	33
3.13 Saving Changes or Resetting Factory Defaults	33
3.14 PPP Net Guardian	34
3.15 DCPx Net Guardian	34
Monitoring Chapter 4	35
4.1 Monitoring the Net Guardian 832A	35
4.1.1 Monitoring Base Alarms	35
4.1.2 Monitoring Ping Targets	36
4.1.3 Monitoring and Operating Relays (Controls)	36
4.1.4 Monitoring Analogs	37
4.1.5 Monitoring System Alarms	37
4.1.6 Monitoring Data Port Activity	38
4.2 Viewing Live Target Pings	39
4.3 Viewing your System Statistics	39
4.4 Proxy menu	40
4.5 LCD Menu	41
4.5.1 Sounds from the Net Guardian 832A	41
4.5.2 Reboot and Forced Configuration	41
4.6 Front panel LED operation	42
4.7 Component Review	43
Appendices	
Display Mapping Appendix A	44
SNMP Manager Functions Appendix B	45
ASCII Conversion Appendix C	47
Customer Support Appendix D	48
Index	50
Notes	52
Warranty	55

Overview

Chapter 1



Fig. 1.1 - Net Guardian 832A monitors alarms, pings network elements, and reports via SNMP, pager or e-mail.

1.1 Summary of Features

Event Notification

- SNMP TRAPS to multiple SNMP managers
- Numeric and Alpha paging
- E-mail
- Local audible and visual
- Support for multiple auxiliary displays (GLDs)

Mediation

- Eight RS232 ports transferred to LAN
- 32 discrete inputs for environmental alarms, equipment alarms, intrusion alarms, etc.
- 32 "PING" alarms, a low level device check for IP aware equipment
- Eight analog alarms with four user defined thresholds set for each input
- Eight relay operated controls for remotely activating standby equipment, locking doors, or any other event that can be triggered by a relay closure or opening
- All managed data is accessible via LAN using any standard SNMP manager or TELNET client
- PPP (dial-in network access) version available for off network sites
- Works seamlessly with DPS Masters T/MonXM or IAM (DCPx version)

Physical

- One rack unit tall and mounts in 19" or 23" rack
- Connectorized back panel (hinged wire wrap back panel or easy connection to 66 blocks available)
- LCD for descriptive display of alarms
- LED indications for alarm and communication status

Access

- Dial-up access
- TELNET over LAN
- Local access with laptop through front panel craft port
- Web browser access (Monitor and provision)

Upgradeability

- Firmware updates are easily downloaded without affecting provisioning information either locally or remotely using NG Loader software
- Feature codes give access to specially ordered features
- Download new firmware remotely using T/MonXM

1.2 Introduction

The Net Guardian 832A is a powerful, compact LAN-based alarm collector that provides network managers with remote visibility of their IP network elements. With 32 ping alarms, 32 discrete alarms, 8 controls, and 8 analogs, this versatile unit is the ideal network monitoring solution. If an element fails to respond to successive pings, or if something is amiss with the environmental controls, the Net Guardian 832A notifies personnel with a complete status message using a variety of methods. Notification types include alphanumeric pager, numeric pager, text message, TCP text, T/MonXM, and E-mail. In addition to network and environmental alarms and controls, the Net Guardian also acts as a terminal server for 8 serial ports, thereby eliminating the need for dedicated circuits and the recurring monthly costs associated with such transports.

The Net Guardian 832A will also report discrete alarms, relay status, analog alarms and network equipment failures over the LAN/WAN to an SNMP manager using SNMP traps (SNMP firmware version). Use the SNMP manager software of your choice to monitor all of the data managed by the Net Guardian. Multiple SNMP managers at multiple IP addresses are also supported. The DCPx firmware version will report to DPS Masters IAM or T/MonXM over LAN.

The Net Guardian 832A is easily provisioned using any web browser or generic TTY terminal. The user-friendly web browser interface or the text-based menus enable the user to quickly set up point descriptions, pager numbers and e-mail addresses of maintenance staff as well as additional options. Provisioning can be done on site, using the front panel craft port, or remotely via LAN or dial-up modem. The entire configuration is saved on the Net Guardian 832A where it remains secure through power outages in non-volatile RAM.

Local visibility of the Net Guardian's status is also accomplished through front panel diagnostic LEDs for alarms and communications, a scrolling LCD menu supplying more detailed information, and audible notification of events.

The Net Guardian 832A is easy to install, with connectors for all serial and LAN ports, alarm, analog and control wiring. Familiar 66 block connections or a hinged back panel with all wire wrap connections are also available for other installation options. It mounts quickly in either 19" or 23" equipment racks while occupying only one rack unit of space. Should the need arise to upgrade the Net Guardian's firmware, simply download the file remotely via LAN using the NGLoader software. The Net Guardian is also easily expandable with capacity for up to three Net Guardian Expansion units providing an additional 48 discrete points per unit for a total of 176 discrete points.

The versatility, capacity, and reliability of the Net Guardian 832A are the reasons why it is the standard solution for network alarm monitoring needs.

Net Guardian 832A Functional Diagram

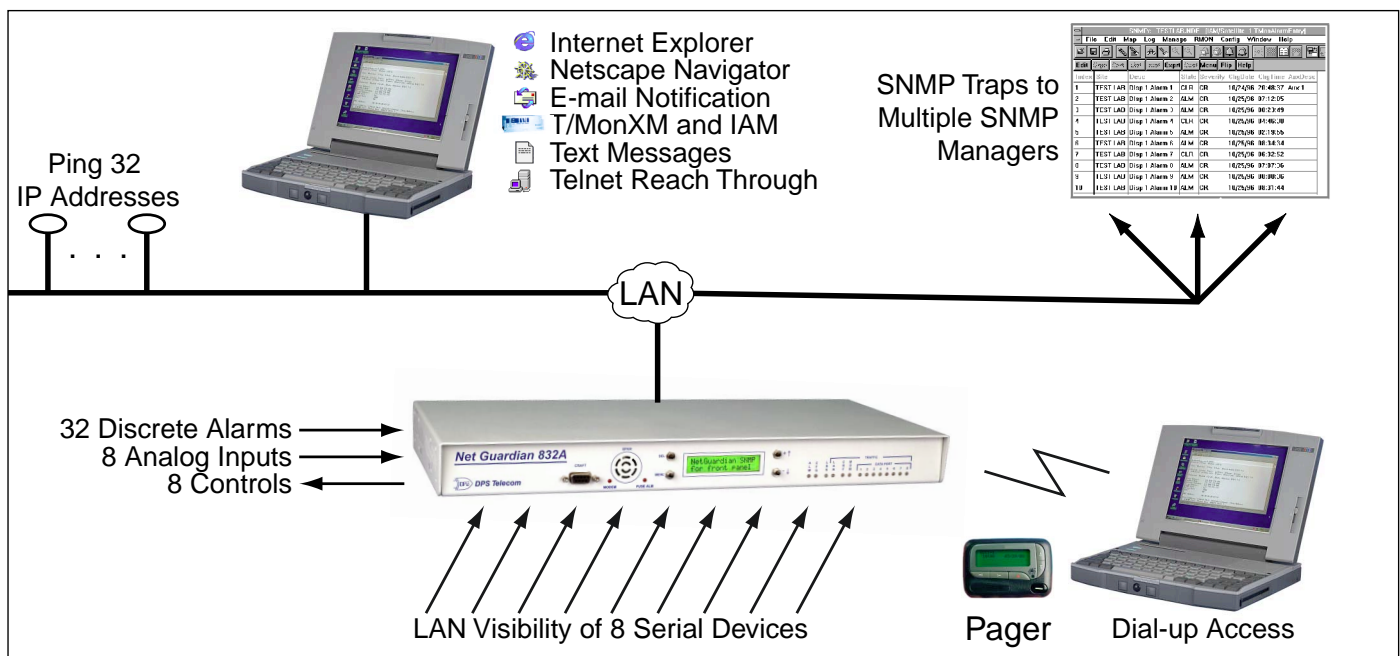


Fig. 1.2 - Net Guardian 832A monitors IP aware devices' network presence as well as interfaces discrete alarm points and controls at your network sites.

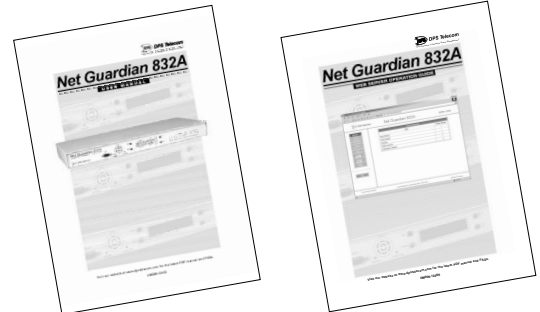
Hardware

Chapter 2

2.1 Shipping List



Net Guardian 832A



**Net Guardian 832A User Manual (UM00A.30230)
Web Server Operation Guide (UM006.12200)**



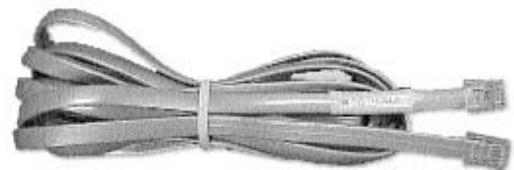
Download Cable 4 ft. (D-PR-045-10A-04)



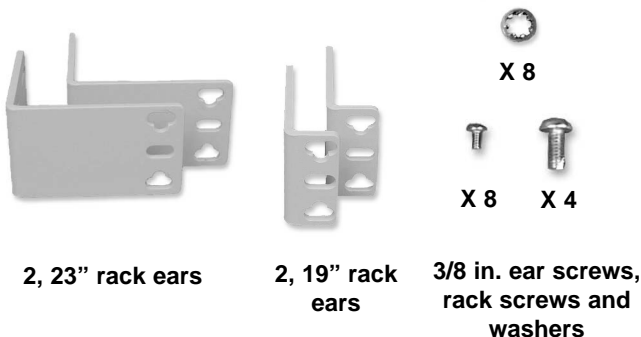
**Ethernet Cable 8 ft. (RJ45 to RJ45)
(D-PR-517-10A-00)**



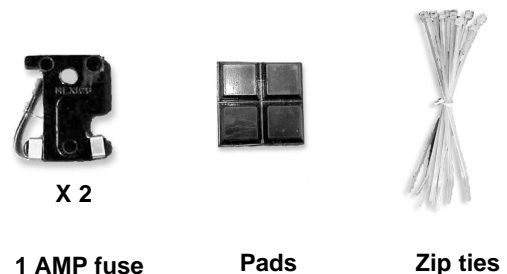
MIB File Disk (D-SW-790-10A-00)



Telephone line Cable (D-PR-045-10A-00)



Mounting Kit



1 AMP fuse

Pads

Zip ties

2.2 Specifications

Net Guardian 832A



Dimensions:	17" W x 12" L x 1.75" H		
Weight:	4 lbs. 3 oz. (1.9 kg)		
Mounting:	19" or 23" rack ears		
Power Input:	-48 VDC unit (-40 to -70 VDC) Wide Range unit (-18 to -70 VDC)	Audible:	Speaker
		Visual:	LCD (descriptive text) LEDs
Current draw:	200mA	Shipping	
Interfaces:	8 DB9 DCE RS232 ports 1 RJ45 Ethernet 10 baseT port 1 RJ11 POTS jack 2 amphenol connectors (alarms, controls, and analogs) 1 DB9 connector (analog)	Box Dimensions:	22" X 6" X 12"
Modem:	33.6K internal	Options:	Net Guardian Expansion units General LCD Display (GLD) support LED bar support Bell box 66 split block
Protocols:	SNMP or DCP (depending on firmware ordering options) TAP (Alpha) paging Numeric paging		
Ctrl Outputs:	Relay contacts, 8 each, form C Max. Voltage = 60 VDC/120 VAC Max. Current = 1 Amp, AC/DC		
Discrete Point Inputs:	32		
Alarm Detection Speed:	User defined (from 3 to 999 msec)		
IP Address Ping Targets:	32		
Analog Alarms:	8		
Input Range:	(-79.9 to 79.9VDC or 4 to 20ma)		
Operating Temperature:	0°- 60°C (32° to 140°F)		
Operating Humidity:	0% to 95% non condensing		
Fuse:	1 Amp GMT		

2.3 Hardware Installation

2.3.1 Site Preparation

Tools needed:

- Phillips screwdriver
- Small standard No. 2 screwdriver
- Laptop with terminal emulation software or a web browser (See Web Server Operation Guide - UM006.12200 for web browser information)
- Wire strippers/cutter
- Wire wrap gun if hinged wire wrap panel is used
- Punch down tool if 66 blocks are used

2.3.2 Installation Steps Overview

1. Review shipping list (Section 2.1).
2. Mount the Net Guardian 832A in the rack (Section 2.3.3).
3. Connect power (Section 2.3.4).
4. Connect communication lines (Section 2.3.5).
5. Connect alarm leads (Section 2.3.6.1).
6. Connect control outputs (Section 2.3.6.2).
7. Connect analog leads (Section 2.3.6.3).
8. Connect data ports (Section 2.3.7).
9. Provision software (Chapter 3).
10. Review Net Guardian 832A's status LEDs and LCD (Sections 4.5 and 4.6).
11. In case of difficulty, contact DPS Tech Support (Appendix D - Customer Support).

2.3.3 Mounting Instructions

The Net Guardian 832A can be mounted in a 19" rack or a 23" rack by using different rack ears for each size (provided). Two rack ear locations are provided. Attach the ears for your rack in the flush-mount or rear-mount locations as shown in the figure below.

Note: Rack ears can be rotated 180° for other mounting options not shown.



Fig 2.3.3 - The Net Guardian 832A can be flush or rear-mounted, as shown above.

2.3.4 Power Connection

1. Remove the fuse from the back panel and turn off the power supply when connecting the power from the power lead.
2. Connect a -48VDC line to the -BATT terminal and the ground to the GND terminal.
3. Turn on main power with the Net Guardian fuse still removed.
4. Connect the black common lead of a volt meter to ground and the red lead to -BATT. The meter should read the battery level (-43 to -53VDC). If not, check your power supply.
5. Do not re-insert the Net Guardian's fuse (powering up the unit) until all other connections have been made.

Note: Observe polarity when connecting battery leads. If using the -48VDC red/black cables supplied with the unit, connect black to GND and red to -BATT. Standard gauge is 20AWG, but may vary between 18-24AWG.

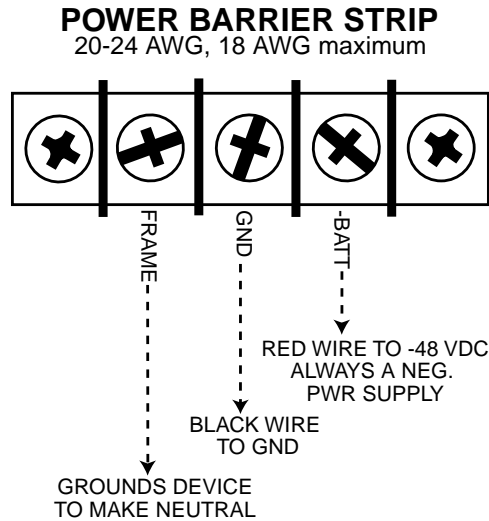


Fig. 2.3.4 - Power Barrier Strip.

2.3.5 Communication Lines

2.3.5.1 LAN Connection

Connect a standard RJ45 Ethernet cable from the local network (LAN) to the 10BaseT jack on the back panel of the Net Guardian 832A (see figure 2.3.5 below). This is used for TELNET access or Web Browser access (see Web Server Operation Guide UM006.12200). See section 3.1.4 for LAN connection information.

2.3.5.2 Phone Line Connection

Connect a standard telephone cable from a POTS line to the RJ11 TELCO jack on the back panel of the Net Guardian 832A. This is used for dial-up access and for paging capabilities (see figure 2.3.5 below).

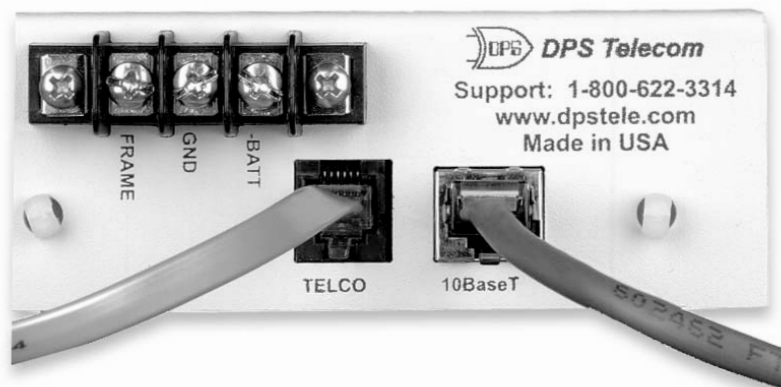


Fig. 2.3.5 - TELCO and 10BaseT ports.

2.3.6 Alarm and Relay connections

Connect discrete alarms, analog alarms, and control points (relays) to the back panel of the Net Guardian via the two Amphenol connectors and the single male DB9 connector. To simplify installation, DPS offers optional Amphenol to open end cables, Amphenol to 66 block, or a hinged back panel with wire wrap terminals for all connections (see section 2.4 for accessory installation information).

2.3.6.1 Discrete Alarms

Discrete alarm points connected to the Net Guardian 832A are essentially single-lead signals referenced to ground. The B-side of each alarm point is internally wired to ground, so either a single wire bringing a contact to ground or a dry closure with the second lead connected to the B-side will be sensed as an alarm signal (see figure 2.3.6.5c for an alarm connection diagram). Typical usage of discrete alarms might include monitoring things such as door alarms, power outages, equipment functionality, etc. Discrete alarms are connected to the two female 50-pin Amphenol connectors located on the back panel. Refer to table 2.3.6 for discrete alarm Amphenol connector pinouts and section 3.7 for discrete alarm software configuration.

2.3.6.2 Control Points (Relays)

The Net Guardian 832A has the ability to control up to eight external devices using relays. Typical functionality of the relays might include starting or stopping equipment, unlocking doors, or other functions. The relay connections are located in the back panel Amphenol connector labeled “Discretes 25-32, Relays 1-8/Analog 1-6.” Pin numbers for each relay are given in table 2.3.6. Refer to section 3.8 for setting the relay parameters and section 4.1.3 for monitoring and operating relays. The relays are set to normally open (N/O) as the default, however, each can be easily changed (via PC board jumpers) to normally closed (N/C) (see section 2.3.8 PCB Settings).

2.3.6.3 Analog Alarm Channels

The Net Guardian 832A allows you to measure either voltage or current on the analog channels. Typical measurements might include battery voltage, charging current, or temperature. Measurements can be made within the voltage range of -79.9 to 79.9 VDC and the current range of 4-20 mA. The default setting is voltage, however each channel can be strapped to include a 250 ohm shunt resistor to measure current. The current through the shunt is analogous to the voltage across it (see section 2.3.8 PCB Settings for jumper locations and positions).

Analog alarm inputs 1-6 are located in the Amphenol furthest to the left side of the back panel. Analog alarm inputs 7 and 8 are located in the male DB9 connector also located on the back panel and labeled “Analog 7-8.” Pin numbers are given in table 2.3.6. Refer to section 3.9 for setting the analog parameters.

Tbl. 2.3.6 - 50 pin Amphenol and analog DB9 pinouts.

Discretes 1-24						Discretes 25-32 Relays 1-8/ Analogs 1-6						DB9 Analogs 7-8		
	B	A		B	A		B	A		B	A		+	-
ALM 1	1	26	ALM 14	14	39	ALM 25	1	26	RLY 6	14	39	ADC 7	6	1
ALM 2	2	27	ALM 15	15	40	ALM 26	2	27	RLY 7	15	40	ADC 8	7	2
ALM 3	3	28	ALM 16	16	41	ALM 27	3	28	RLY 8	16	41			
ALM 4	4	29	ALM 17	17	42	ALM 28	4	29	FUSE	17	42			
ALM 5	5	30	ALM 18	18	43	ALM 29	5	30	N/A	18	43			
ALM 6	6	31	ALM 19	19	44	ALM 30	6	31		+	-			
ALM 7	7	32	ALM 20	20	45	ALM 31	7	32	ADC 1	19	44			
ALM 8	8	33	ALM 21	21	46	ALM 32	8	33	ADC 2	20	45			
ALM 9	9	34	ALM 22	22	47	RLY 1	9	34	ADC 3	21	46			
ALM 10	10	35	ALM 23	23	48	RLY 2	10	35	ADC 4	22	47			
ALM 11	11	36	ALM 24	24	49	RLY 3	11	36	ADC 5	23	48			
ALM 12	12	37	GND	25	50	RLY 4	12	37	ADC 6	24	49			
ALM 13	13	38				RLY 5	13	38	GND	25	50			

2.3.6.4 Connecting alarms with a 66 block

Each 50 pin Amphenol on the Net Guardian back panel can be connected to a 66 block (25 pair block) (Part number D-PR-966-10A-00). See figure 2.3.6.4a for pinout and color code information for Discretes 1-24 and figure 2.3.6.4b for pinout and color code information for Discretes 25-32, Relays 1-8, and Analogs 1-6. See section 2.3.6 for alarm and relay connection information.

Note: If connecting to a 50 pair split block, all connections should be made on the 2 pin columns closest to the right hand side of the block.

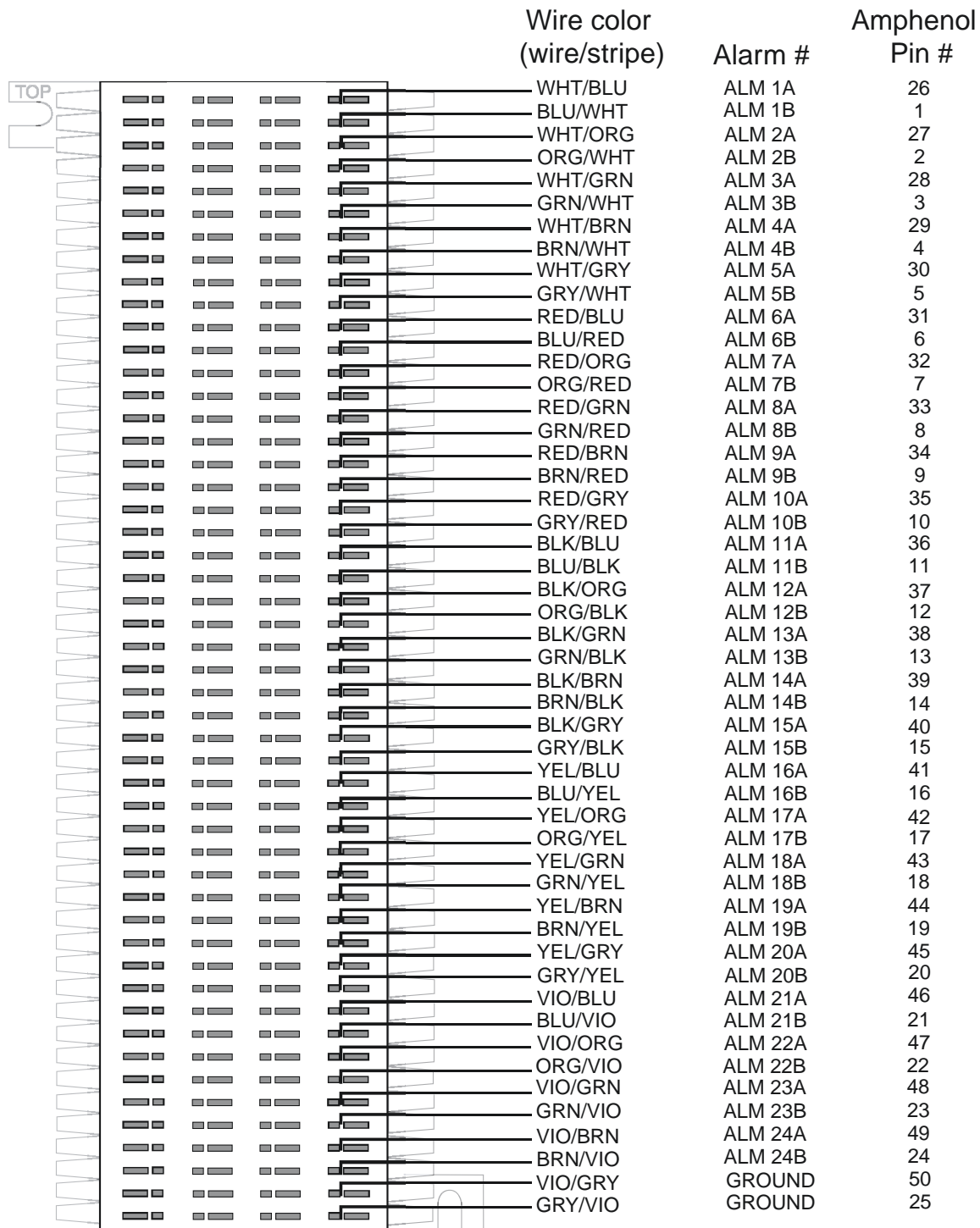


Fig. 2.3.6.4a - 66 Block (D-PR-966-10A-00) for Discretes 1-24.

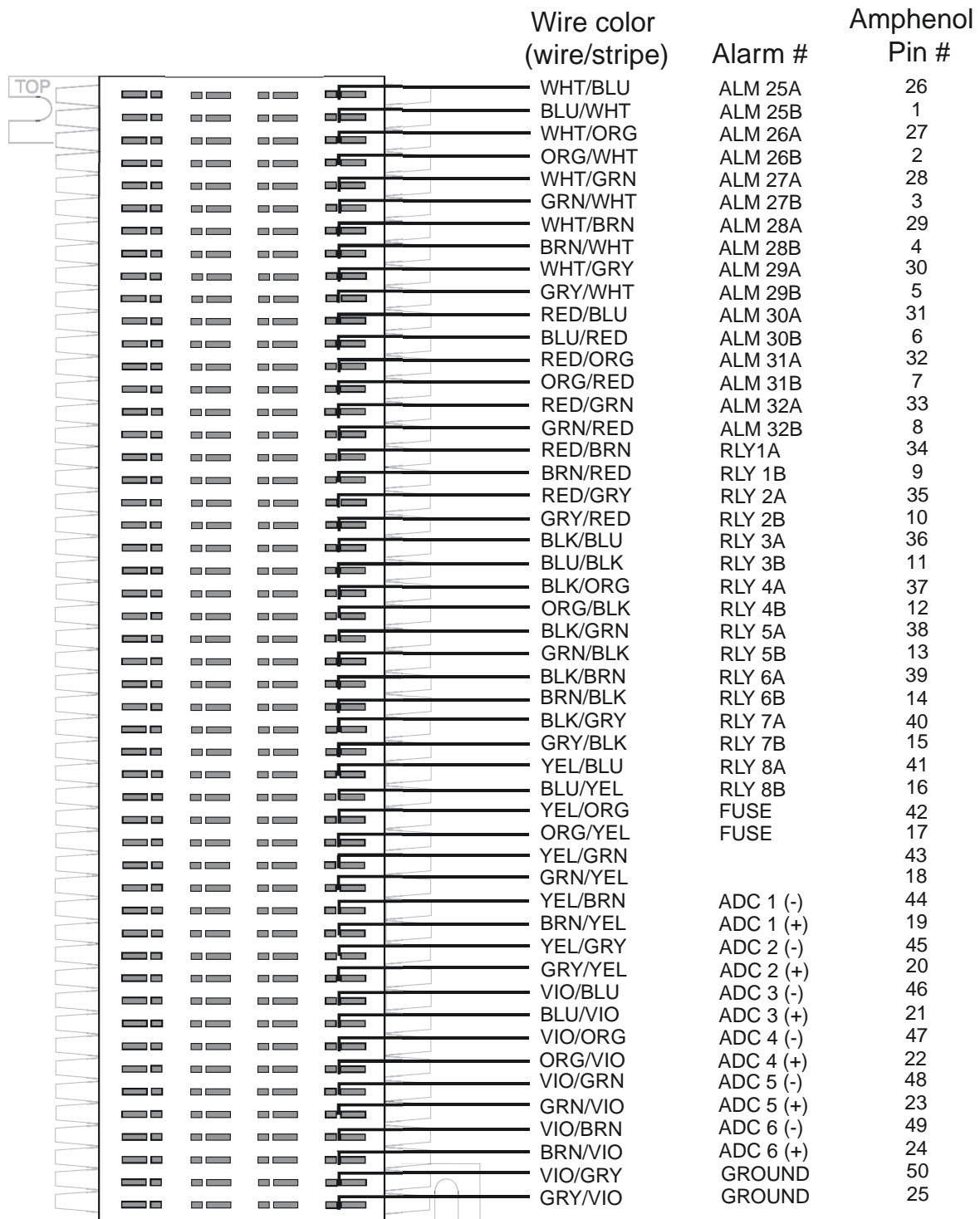


Fig. 2.3.6.4b - 66 Block for Discretes 25-32, Relays 1-8, and Analogs 1-6.

2.3.6.5 Net Guardian 832A Back Panel

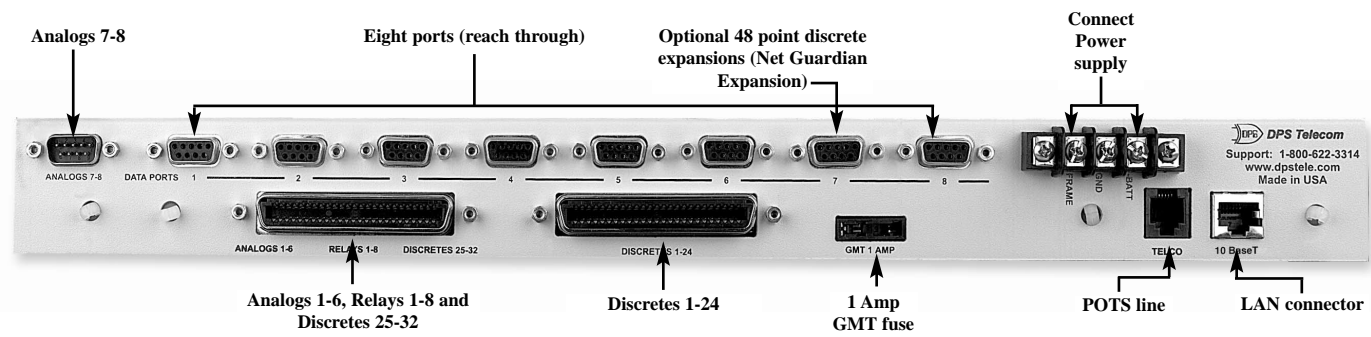
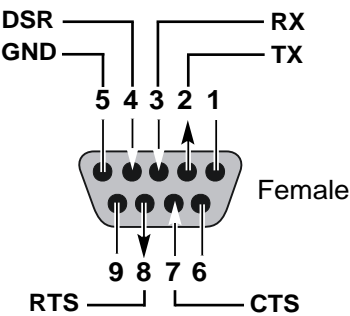


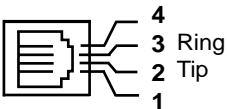
Fig. 2.3.6.5a - The Net Guardian back panel has eight DB9 DCE type serial ports, two 50-pin Amphenol™ alarm/control/analog connectors, one DB9 analog connector, one RJ45 jack for LAN, one RJ-11 jack for a telephone line, and a power barrier strip.

Eight rear panel Serial ports and the front panel Craft port - Female DB9



PIN#	Signal	Description
1	NC	Not connected
2	TX	Transmit data
3	RX	Receive data
4	DSR	Data set ready
5	GND	Ground
6	NC	Not connected
7	CTS	Clear to send
8	RTS	Request to send
9	NC	Not connected

Phone line
Connection RJ-11



LAN
Connection RJ-45

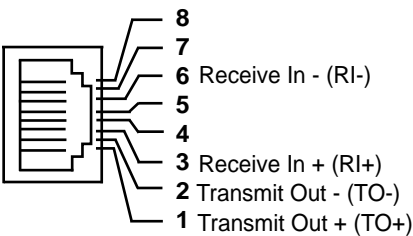


Fig. 2.3.6.5b - Serial, phone and LAN communication ports are located on the rear of the Net Guardian 832A.

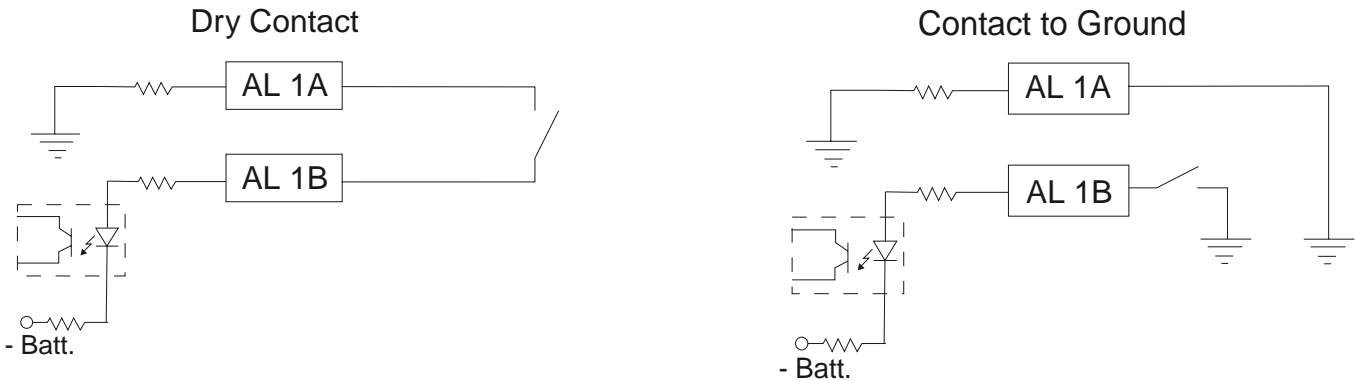


Fig. 2.3.6.5c - Discrete alarm points can connect as a dry contact or a contact to ground.

2.3.7 Data Ports (reach-through)

Connect up to eight devices with an RS232 serial interface to the DB9 RS232 DCE data ports on the back panel. If connecting a Net Guardian Expansion unit, use port 7. If connecting a General LCD Display (GLD) unit, use port 8. The data ports also serve as proxy connections for other devices. Additionally, each port can also function as a craft port, a channel port, TCP reach-through port, or UDP reach-through port. See section 3.5.5 for data port configuration information and a description of each functionality option. Multiple users may establish proxy connections (reach through the Net Guardian) simultaneously via Telnet sessions over LAN to a group of 8 “proxy” ports defined later in the software provisioning section. See figure 2.3.6.5b for DB9 pinout information.

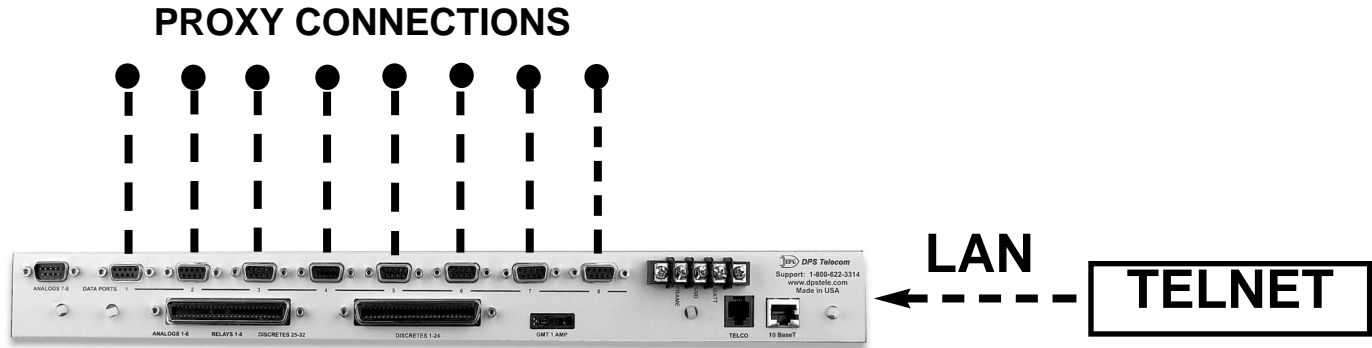


Fig. 2.3.7 - The Net Guardian 832A supports concurrent proxy connections for multiple users to TELNET into different ports/devices.

2.3.8 PCB Settings

Certain analog alarm configurations and relay operations require alternate jumper settings. Refer to section 3.9 - Setting the Analog Parameters and section 4.1.3 - Monitoring and Operating Relays for specific jumper setting information. To open the unit and expose the circuit board, remove the screws from the sides of the Net Guardian and remove the amphenol hex screws from the rear panel, then lift the case lid up as shown below.

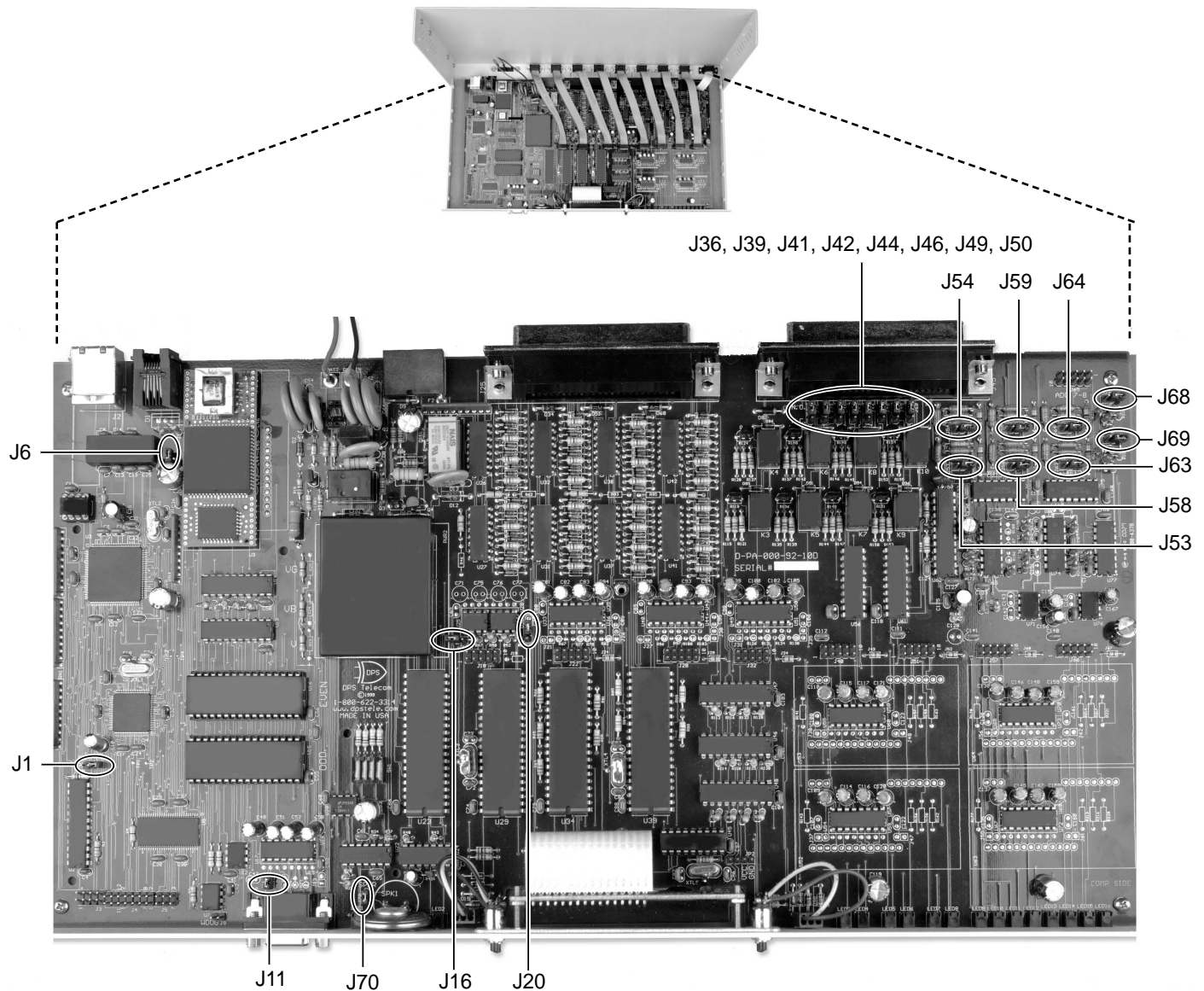


Fig. 2.3.8a - Net Guardian 832A circuit board with jumpers labeled.

Current

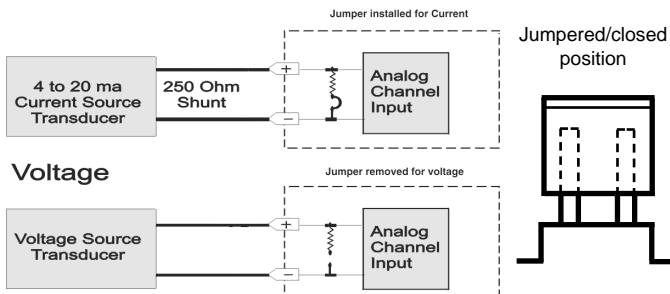


Fig. 2.3.8b - Each analog alarm input can be switched to measure current instead of voltage by changing its jumper position.

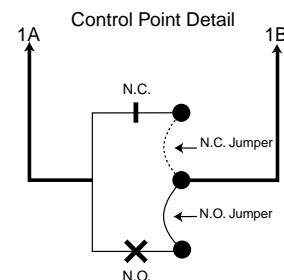


Fig. 2.3.8c - Each relay can be switched to normally closed by changing its jumper position.

Tbl. 2.3.8 - Net Guardian 832A PCB settings.

PCB Ref. #	Default Position	Description
J1	Open	Factory Use.
J6	Open	Factory Use.
J9	Open	Factory Use.
J11	Closed (Do not remove)	Craft port ground.
J36	N.O.	Relay 1.*
J39	N.O.	Relay 2.*
J41	N.O.	Relay 3.*
J42	N.O.	Relay 4.*
J44	N.O.	Relay 5.*
J46	N.O.	Relay 6.*
J49	N.O.	Relay 7.*
J50	N.O.	Relay 8.*
J53	Voltage (Open)	Analog alarm 2.**
J54	Voltage (Open)	Analog alarm 1.**
J58	Voltage (Open)	Analog alarm 3.**
J59	Voltage (Open)	Analog alarm 4.**
J63	Voltage (Open)	Analog alarm 6.**
J64	Voltage (Open)	Analog alarm 5.**
J68	Voltage (Open)	Analog alarm 8.**
J69	Voltage (Open)	Analog alarm 7.**
J70	Closed	Speaker is disconnected when open.

* To change a relay to be normally closed (N.C.), place the corresponding circuit board jumper in the N.C. position (See figure 2.3.8b)

** To change the analog input to measure current (range of 4 to 20 mA), place the jumper in the closed position (See figure 2.3.8b)

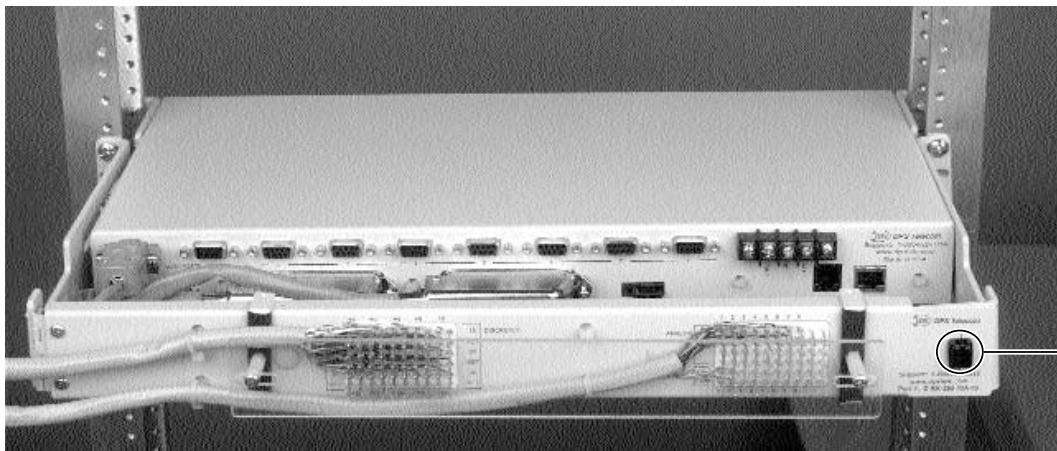
2.4 Net Guardian Accessory Installation

There are various accessories available for the Net Guardian. These include the hinged wire wrap back panel, 66 Block (Solid and Split), LED bar, bell box and General LCD Display (GLD). For more information on these products or to place an order, please call 1-800-622-3314.

Note: Not all accessories are available for all Net Guardians. Some accessories have firmware and hardware prerequisites. Check the specific accessory user manual for the Net Guardian minimum version requirements.

2.4.1 Hinged wire wrap back panel

- 1). Mount the hinged wire wrap back panel on the Net Guardian rack. (See figure 2.4.1a)
- 2). Close the hinged back panel and lock in place by turning the black plastic locking mechanism to the vertical position. (See figure 2.4.1a).
- 3). Connect discrete alarms, analog alarms, and control points (relays) to the two pin blocks. Refer to section 2.3.6 for alarm and relay connection information and figures 2.4.1a and 2.4.1b for wire wrap pinout information.



Turn the plastic swivel to the vertical position to lock in place

Fig. 2.4.1a - Mount the hinged back panel on the mounting rack of the Net Guardian.

2.4.1.1 Plexi-glass wire-wrap cover

- 1). Before connecting communication wires, attach the mounting clips to the rear panel of the hinged back panel.
- 2). After attaching communication wires, mount the plexi-glass cover by inserting the screws into the mounting clips.

		+0	+2	+4	+6	+8	
Discretes 1 - 10	1	10
(Return 1 - 10)	RET	RET
Discretes 11 - 20	11	20
(Return 11 - 20)	RET	RET
Discretes 21 - 30	21	30
(Return 21 - 30)	RET	RET
		+0	+2	+4	+6	+8	

Fig. 2.4.1.1b - Wire-wrap pinouts for discrete alarm 1-30.

		+0	+2	+4	+6	+8	
Analogs 1 - 8	+	
	-	
Discretes 31 - 32		
(Return 31 - 32)		
Controls 1 - 8	N/O	
	COM	
		+0	+2	+4	+6	+8	

Fig. 2.4.1.1c - Wire-wrap pinouts for discrete alarms 31-32, analogs 1-8, and controls 1-8.

Software Provisioning

Chapter 3

3.1 Connecting to the Net Guardian

The Net Guardian 832A must be provisioned for port configurations, alarm and relay definitions, and network address information before operation can begin. This is accomplished by navigating through text based menus over a terminal attached to the craft port, through a remote dial-up connection, or through a telnet session via LAN. Alternatively, a Web Browser may also be used. However, initial setup of the Ethernet port must be done through the front panel craft port before Telnet sessions and the web interface can be used. For information regarding provisioning steps and operation through the Web Browser interface of the Net Guardian 832A, see the Web Server Operation Guide (UM006.12200).

3.1.1 Web Server

For Web Server configuration and operation, see the Net Guardian Web Server operation guide (UM006.12200).

3.1.2 Local Connection

Connect a PC running terminal emulation software to the craft port on the front of the Net Guardian 832A using a DB9 download cable (provided) (See figure 3). Set your serial port to match the data rate and word format currently defined for the Net Guardian 832A (factory default is 9600 N, 8, 1). Also in your terminal emulation software, set the Flow control to “None.” When a connection is established (sometimes accompanied by receipt of a hex byte), type DPSCFG <Enter> to activate the configuration menu.

Note: Menu selection Hot Keys: The letters before a parentheses or enclosed in parentheses () are hot keys. Press the hot key to access that submenu. Pressing the <Esc> key will always bring you back to the previous level. Entries are not case sensitive.

3.1.3 Remote Connection (Dial Up)

Set up a PC running TTY terminal emulation (Telnet) software to dial the Net Guardian 832A’s modem. When a connection is established (sometimes accompanied by receipt of a hex byte), type DPSCFG <Enter> to activate the configuration menu.

Note: If the system has been previously configured, it might be set for “quiet login”, which is part of the security system. Enter your login data without prompting until you are logged on.

3.1.4 LAN Connection

You can connect to the Net Guardian 832A using any standard TELNET client or web browser, but the Ethernet port must first be configured. Refer to section 3.1 for initial LAN/WAN setup steps. For TELNET, connect to the Net Guardian’s IP address at port 2002 to access the configurator menus after initial LAN/WAN setup. TELNET sessions are established at port 2002, not the standard TELNET port, as an added security measure. For web browser connections, enter the IP address of the Net Guardian into the web browser’s address bar and refer to the Web Server Operation Guide (UM006.12200).

Note: For networks utilizing a DHCP server, a fixed IP address is recommended for the Net Guardian to provide a consistent location for web browser access.



Fig. 3 - Connect to the craft port to configure the Net Guardian 832A.

3.2 LAN/WAN setup

Initially, the Net Guardian 832A must be provisioned with an appropriate IP address before you will be able to connect via LAN/WAN using a TELNET client or a web browser. This must be done using the front panel craft port .

1. Ensure your Terminal Emulation software connection settings match the Net Guardian 832A's (9600, N, 8, 1, also set Flow Control to None—not Hardware) and connect to the DB9 connector of the front craft port.
2. Type: 'DPSCFG' <enter>
3. The Net Guardian 832A's will respond with Password:
4. Type: 'dpstelecom' <enter> (Factory default)
5. The Net Guardian 832A's main menu will appear.
6. Type 'C' for configure.
7. Type 'E' for edit.
8. Type 'P' for port.
9. Type 'E' for ethernet port.
10. Enter the unit address, subnet mask, default gateway, trap address, SNMP port number, proxy base port and DHCP option. Press ESC twice to back up two menus.
11. Go to n(V)ram and W)rite the configuration to memory, then enter ESC.
12. Go to the s(Y)stem menu and R) reboot. Type 'y' to reboot. This will load the saved configuration.
13. Now you can connect over LAN to complete the configuration, or configure the unit using the current connection.

Note: The LAN minimum configuration requires setting the Unit Address (IP) and the Subnet Mask. Use of a WAN requires that the Default Gateway be set as well.

```

Password: *****

NetGuardian SNMP v2.1B.0712
C)onfig P)roxy D)ebug e(X)it

E)dit M)onitor P)ing S)tats R)eset modem (ESC) ? E

s(Y)stem L)ogin P)orts pa(G)ers A)larms R)elays
  a(N)alog s p(I)ng info T)imers D)ate/time n(V)ram (ESC) ? P

E)thernet M)odem C)raft D)ata O)ptions (ESC) ? E

Unit Address      : 126.010.220.199
SubNet Mask       : 255.255.255.000
Default Gateway   : 126.010.220.001
Trap Address      : 126.010.220.198
SNMP Port         : 162
Proxy Base        : 3000
DHCP              : NO
Base URL          : www.dpstele.com/&pntID;.pdf

MAC Address       : 00.10.81.00.03.59

U)nit Address S)ubnet Mask D)efault Gateway T)rap Address
S(N)MP Port P)roxy Base D(H)CP B)ase URL (ESC) ?

```

Fig. 3.2 - Configure the Ethernet port parameters to connect via LAN/WAN.

Note: See Table 3.5.1 for detailed field descriptions for the screen above.

3.3 Entering System Settings

After configuring the Ethernet port, go to s(Y)stem and set up the N(ame), L(ocation), and C(ontact) information.* TELNET sessions are established at port 2002, not the standard TELNET port, as an added security measure.

* The name and location fields are also used for e-mail paging functions as the “from” address in e-mail messages in the format of “name@location”. For specific instructions on configuring the e-mail paging function, see section 3.6.1.

```

Password: *****

NetGuardian SNMP v2.1B.0712
C)onfig P)roxy D)ebug e(X)it

E)dit M)onitor P)ing S)tats R)eset modem (ESC) ? E

s(Y)stem L)ogin P)orts pa(G)ers A)larms R)elays
a(N)alogs p(I)ng info T)imers D)ate/time n(V)ram (ESC) ? Y

Name           : Net Guardian 832A
Location       : 4955 E. Yale Fresno, CA 93727
Contact        : DPS Telecom 1-800-622-3314
Features       : D0CB-53-0C5C
Communities
  Get          : public
  Set          : public
  Trap         : public

N)ame L)ocation C)ontact F)eatures
A)larms G)et S)et T)rap R)eboot (ESC) ?

```

Fig. 3.3 - The system information describes the unit.

Tbl. 3.3- System Submenu Fields.

FIELD	DESCRIPTION
Name	User designated name for this Net Guardian 832A (also used for portion of “from” address in e-mail notification of alarms).
Location	Physical location of Net Guardian 832A (also used for portion of “in” address in e-mail notification of alarms).
Contact	Person responsible for this Net Guardian 832A.
Features	Used for entering feature codes for future upgrade features.
Get	Community name for SNMP requests.
Set	Community name for SNMP SET requests.
Ttrap	Community name for SNMP TRAP requests.

3.4 Changing the Logon Password

The password parameters can be changed using the L)ogin menu selection. Password length, the actual password and “quiet login” can be configured.

1. Enter your desired minimum password length. The minimum password length is 1 character, however, for security reasons, DPS recommends a minimum password length of at least 5 characters.
2. Enter your password.
3. Enter “YES” or “NO” for Quiet Login. This determines whether or not the “Password:” prompt appears when the user initially connects to the system. This provides a degree of security when the value is set to “yes”. An unauthorized user will have no way of knowing that the Net Guardian 832A is expecting a password input, since no characters are displayed on the screen.

```
E)dit  M)onitor  P)ing  S)tats  R)eset modem (ESC) ? E

s(Y)stem  L)ogin  P)orts  pa(G)ers  A)larms  R)elays
  a(N)alog  p(I)ng info  T)imers  D)ate/time  n(V)ram (ESC) ? L

Minimum password length : 5
          Password : *****
          Quiet login : YES

M)inimum password  P)assword  Q)uiet connect (ESC) ?
```

Fig. 3.4 - Define a new password in the L)ogin menu.

3.5 Configuring Port Parameters

Selecting E)dit followed by P)orts takes you to the ports configuration menu. From here you can change values for the E)thernet, M)odem, C)raft, and D)ata ports.

3.5.1 Ethernet Ports

Going from the E)dit menu to the P)ort menu, to the E)thernet selection displays the screen below. Each of the parameters: U)nit Address, S)ubnet Mask, D)efault Gateway, T)rap Address, S(N)MP Port, P)roxy Base, and B)ase URL can be changed to the values provided by your network administrator. The fields are explained in table 3.5.1.

```
s(Y)stem L)ogin P)orts pa(G)ers A)larms R)elays
a(N)alogs p(I)ng info T)imers D)ate/time n(V)ram (ESC) ? P

E)thernet M)odem C)raft D)ata O)ptions (ESC) ? E

Unit Address      : 126.010.220.199
SubNet Mask       : 255.255.255.000
Default Gateway   : 126.010.220.001
Trap Address      : 126.010.220.198
SNMP Port         : 162
Proxy Base        : 3000
DHCP              : NO
Base URL          : www.dpstele.com/&pntID;.pdf

MAC Address       : 00.10.81.00.03.59

U)nit Address S)ubnet Mask D)efault Gateway T)rap Address
S(N)MP Port P)roxy Base D(H)CP B)ase URL (ESC) ?
```

Fig. 3.5.1 - Configure the Ethernet Port for LAN/WAN use.

Tbl. 3.5.1 - Field descriptions for the Ethernet Ports submenu.

FIELD	DESCRIPTION
Unit Address	IP address of the Net Guardian 832A.
Subnet Mask	A road sign to the Net Guardian 832A telling it whether your packets should stay on your local network or be forwarded somewhere else on a wide area network.
Default Gateway	An important parameter if you are on a network that is connected to a wide area network. It tells Net Guardian 832A which machine is the gateway out of your local network. Set to 255.255.255.255 if not using.
Trap Address	When an alarm occurs that is marked for setting a trap, it will then send that SNMP trap to the trap address. Set to 255.255.255.255 if not using.
SNMP Port	The SNMP port is the port set by the SNMP manager to receive Trap messages, usually set to 162.
Proxy Base	Defines the TCP ports used by data ports 1-8 (RS 232 serial ports) during proxy connections. Data port 1 receives the port number entered here. Data ports 2-8 receive the next 7 port numbers in ascending order i.e. TCP port 3000 through port 3007.
DHCP	Toggles the Dynamic Host Connection Protocol On or Off. If web browser access is a desired interface, DPS recommends that the DHCP option be turned OFF and a permanent IP address assigned to the Net Guardian to provide a consistent location for web browser access.
Base URL	Destination address of the alarm point description hyperlinks (See section 3.5.1.1).

3.5.1.1 Using the Base URL Field

The Net Guardian 832A allows users to turn specific alarm point descriptions into hyperlinks (Net Guardian Web Server* required to view link - See Web Server Operation Guide UM006.12200). When utilized, the alarm description for each alarm point that appears in the monitor mode (for Base Alarms, Ping Targets, or System Alarms) can be turned into a link that directs technicians/managers to specific web pages (or to other files viewable via a Web Browser). This allows users to create easily accessible informational databases on how to handle specific alarm conditions or other instructions. The hyperlinked page or file will be displayed in the main window frame of the Net Guardian Web Browser. Follow the directions below to create hyperlinks for alarm point descriptions.

1. Enter your base URL (e.g. <http://www.dpstele.com>). The Net Guardian creates the links from the alarm point descriptions based on the URL. Once the base URL is entered, the Net Guardian automatically attaches a unique suffix to each alarm point. For example, if the base URL is “<http://www.dpstele.com>”, the link for the Base Alarm at point 1 would be “<http://www.dpstele.com/base1.html>”. (Base Alarm point 2 would be “<http://www.dpstele.com/base2.html>”, etc.)
2. To add a suffix other than “html” to the hyperlinks, insert the text “&pntID;” into the base URL. This allows the user to specify the extension. For example if the base URL is “<http://www.dpstele.com/&pntID;.pdf>”, the link for the Base Alarm at point 1 would be “<http://www.dpstele.com/base1.pdf>”. Any file type that is viewable in your Web Browser (e.g. word document, PDF, txt, etc.) is a linkable file.
3. The same link structure applies to the Ping Alarms and System Alarms fields.

3.5.2 MIB Installation

To enable your SNMP manager to receive and interpret the TRAPs sent by the Net Guardian 832A, the MIB (Management Information Base) file, provided on a floppy disk with the Net Guardian 832A, must be compiled into the SNMP manager’s MIB. The MIB file includes fields for SNMP Trap points, Identity, Displays, Controls, NVRam, and Alarms. MIB objects include setting controls, setting time, viewing alarms, etc. (See Appendix B - SNMP Manager Functions for a complete list of MIB objects and for specific MIB object identifiers). Refer to your SNMP manager’s operating manual or your SNMP support group for instructions regarding this procedure.

Note: The SNMP manager requires correct input of its IP address into the Net Guardian for traps to be deliverable.

3.5.3 Setting Modem Port Values

The modem port ring count parameter can be changed by selecting the M)odem option from the ports menu. This parameter defines the number of rings before answering (Default = 1). The “Dial Init” and the “Answer Init” fields can be used if any other modem initialization settings need to be set. For example, the modem can be set to ignore the dial-tone by entering a character code (refer to a standard modem command (Hayes) reference book for standard commands) in either the Answer Init (in to the Net Guardian) or the Dial Init (out from the Net Guardian). The default setting for these fields is blank (N/A). The R)eset modem selection can be used to reset the modem (e.g. if a call was dropped by the remote party, the modem isn’t responding, etc.)

```

E)dit  M)onitor  P)ing  S)tats  R)eset modem (ESC) ? E

s(Y)stem  L)ogin  P)orts  pa(G)ers  A)larms  R)elays
  a(N)alogs  p(I)ng info  T)imers  D)ate/time  n(V)ram (ESC) ? P

E)thernet  M)odem  C)raft  D)ata  (ESC) ? M

Ring Count : 1
Answer Init :
Dial Init :

R)ing count  A)nsver Init  D)ial Init (ESC) ?

```

Fig. 3.5.3 - Viewing and changing the Modem Port parameters.

3.5.4 Changing Craft Port Communication Settings

The craft port parameters, baud and word format, can be accessed by choosing C)raft from the P)ort menu. Table 3.5.4 provides the possible choices for craft port data rate and word format. Selecting <ESC> twice will return you to the E)dit menu.

Note: *You must reboot the unit for the attribute changes to take effect.*

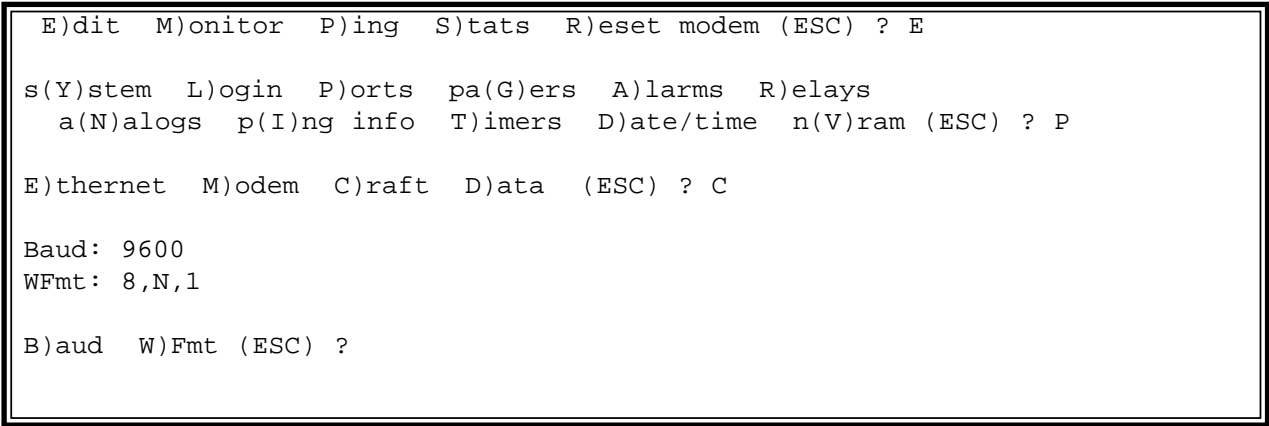


Fig. 3.5.4- *Viewing and changing the craft port UART parameters.*

Tbl. 3.5.4 - *Craft Port Submenu Fields.*

Field	Description
Baud	Port Data Rate (300, 1,200, 2,400, 4,800, 9,600) The default baud is 9,600.
Wfmt	Port Word Format: The default is 8,N,1. Data Bits: Seven or Eight. Parity: None, Even, or Odd. Stop Bits: One

3.5.5 Setting Data Port Values

The D)ata port menu allows you to view and change the parameters for each of the eight data ports. The ports can each be configured for type, Baud rate*, word format and to ignore or remove CR/LF (carriage return/ line feed) characters in either the input or output data stream. Enter a description for each port with a connected device. Each data port may be configured to function as a craft port, channel port, TCP reach-through port, or a UDP reach-through port. If connecting a Net Guardian Expansion unit, use port 7, if connecting a General LCD Display (GLD) use port 8. See figure 3.5.5 for type descriptions.

*The baud rate for the bridged channel pairs (See table 3.5.5 for description) may be set in any combination except 19200 and 38400.

s(Y)stem	L)ogin	P)orts	pa(G)ers	A)larms	R)elays	
a(N)alogs	p(I)ng	info	T)imers	D)ate/time	n(V)ram (ESC) ? P	
E)thernet	M)odem	C)raft	D)ata	O)ptions	(ESC) ? D	
CR/LF Mode						
ID	Description	Baud	WFmt	In	Out	Type
1	ASCII Device	9600	8,N,1	ignore	ignore	CHAN
2	DCP Device	9600	8,N,1	ignore	ignore	CHAN
3	Monitor RS232	9600	8,N,1	ignore	ignore	CRFT
4	Monitor RS232	9600	8,N,1	ignore	ignore	UDP
5	DDM2000	9600	8,N,1	ignore	ignore	UDP
6	Router 1	9600	8,N,1	ignore	ignore	UDP
7	NG Expansion	9600	8,N,1	ignore	ignore	TCP
8	GLD	9600	8,N,1	ignore	ignore	CRFT
Port ID: 1						
CR/LF Mode						
ID	Description	Baud	WFmt	In	Out	
1	Monitor RS232	9600	8,N,1	ignore	ignore	
D)escription B)aud W)Fmt I)n O)ut (ESC) ?						

Fig. 3.5.5 - Viewing and changing data port parameters.

Tbl. 3.5.5 - Data port type descriptions.

Type	Description
TCP	Makes reach-through available at TCP ports (Telnet).
UDP	Makes reach-through available at UDP ports (reserved for future use).
CHAN	Creates logical bridge to odd/even partner. The odd/even partners are pairs of 1-2, 3-4, 5-6, and 7-8. This allows the Net Guardian to view communication traffic in either direction when inserted in the serial communication path between two devices. This is accomplished by going “in” to the Net Guardian with one device and “out” to the other device from the odd/even partner port. Data is passed directly from one port to its odd/even partner without being altered in any way. This ability greatly simplifies troubleshooting communication problems by isolating the non-communicating device. Refer to figure 4.1.6b for a connection diagram.
CRFT	Causes the data port to have the same functionality as the front panel craft port*.

* Baud rates for the odd/even pairs can be set to any available rate except for any combination of 19200 and 38400 between the two ports.

3.6 Setting Up Notification Methods from the Pagers Screen

Selecting pa(G)ers from the E)dit menu displays the current parameters for the pagers. The type of pager (alpha, numeric, text, T/Mon, e-mail, SNMP, or TCP); phone number; PIN/Rcpt/Port; baud rate and word format can all be viewed and selected from within this submenu. The pagers menu is an important menu because it is where several alarm notification types are configured, not just pagers. E-mail notification and multiple SNMP managers are defined here and then selected in alarm point provisioning screens as the primary or secondary pager notified in an alarm condition.

E)dit M)onitor P)ing S)tats R)eset modem (ESC) ? E					
s(Y)stem L)ogin P)orts pa(G)ers A)larms R)elays					
a(N)alogs p(I)ng info T)imers D)ate/time n(V)ram (ESC) ? G					
ID	Type	Phone/Domain	PIN/Rcpt/Port	Baud, WFmt	IPA
1	A	(559) 555-5555	516498	1200,7,E,1	
2	N	(559) 555-5555	461894	1200,7,E,1	
3	T	(559) 555-5555	441629	1200,7,E,1	
4	N	(559) 555-5555	956154	1200,7,E,1	
5	E	domain.com	username	1200,7,E,1	255.255.255.255
6	S	domain.com	username	1200,7,E,1	255.255.255.255
7	Off			1200,7,E,1	255.255.255.255
8	Off			1200,7,E,1	255.255.255.255
Pager ID:					
1	Off			1200,7,E,1	255.255.255.255
T)ype P)hone/Domain P(I)N/Rcpt/Port B)aud W)Fmt IP(A) (ESC) ?					

Fig. 3.6 - Viewing and changing the pager parameters.

Tbl. 3.6- Pager field descriptions.

Field	Description
ID	Identification Number of Pager. The pager IDs are used in the alarm screen to designate who will be paged when an alarm condition is detected by Net Guardian 832A. All information on the pager screen may be changed by typing the ID number <Enter> then use the submenu to change any screen item for that pager.
Type	<p>O - Off (Disabled)</p> <p>A - Alpha numeric Pager</p> <p>N - Numeric</p> <p>T - Text: Send a message in "raw" text to report to computers over a terminal or generic monitoring application.</p> <p>M - T/MonXM: Uses the same DialUp protocol as AlphaMax, DPM and KDA (TRIP)</p> <p>E - E-mail: alarm notification via e-mail.</p> <p>S - SNMP: multiple SNMP managers can be defined to be notified for different alarms.</p>
Phone/Domain	<p>Pager Phone number - used for Alpha, Numeric, Text, and TMon pager types</p> <p>Domain - used for e-mail pager types. The domain name is the portion of an email address that follows the "@" symbol in user@domain.com. The domain field is not used for SNMP pager types. (It may be used as a description field in that case however).</p>
Pin/Rcpt/Port	<p>PIN: used for entering personal identification number for alpha and TMon pager types.</p> <p>Rcpt: enter the recipients name for e-mail pager types here. This is the portion of an e-mail address before the "@" symbol.</p> <p>Port: set the SNMP port in this field.</p>
Baud	Pager Data Rate (300, 1200, 2400, 9600). The default baud is 1200.
Wfmt	<p>Pager Word Format The default designation is 7, E, 1.</p> <p>Data Bits: Seven or Eight Parity: None, Even or Odd Stop Bits: One</p>
IPA	Enter the IPA address of the mail server for e-mail pager types, for SNMP pager types, enter the IP address of the computer to receive the Traps.

3.6.1 Alpha numeric pager setup

The alpha numeric pager can receive text messages including alarm descriptions, time of occurrence, and point addresses.

1. From the pa(G)ers menu (See figure 3.6), enter an ID number of the pager. Pager IDs are used in the alarm provisioning screen to designate the primary and secondary person/device being paged. See figure 3.6.1 for pager description information.
2. Enter type “A” for Alpha numeric paging under the “Type” heading.
3. Enter the phone number of the Alpha numeric pager under the “Phone/Domain” heading.
4. Enter a personal identification number under the “PIN/Rcpt/Port” heading.
5. Set the pager data rate (i.e. 300, 1,200, 2,400 or 9,600). The default baud is 1,200.
6. Select a pager word format (i.e. Data bits: 7 or 8, Parity: none (N), even (E) or odd (O), and Stop Bits: 1). The default setting is 7,E,1.

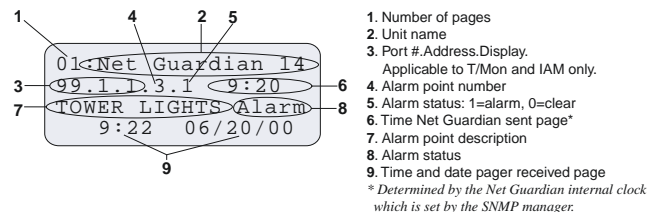


Fig. 3.6.1 - Alpha numeric pager description.

3.6.2 Numeric pager setup

The numeric pager can receive point addresses of alarms.

1. From the pa(G)ers menu (See figure 3.6), enter an ID number of the pager. Pager IDs are used in the alarm provisioning screen to designate the primary and secondary person/device being paged.
2. Enter type “N” for numeric paging under the “Type” heading.
3. Enter the phone number of the numeric pager under the “Phone/Domain” heading, followed by 7 commas (e.g. “555-1212,,,,,,”). Placing a comma after the phone number initiates a 2 second pause (per comma). This allows enough time for the pager to answer and the message to be heard before the Net Guardian sends the alarm.

3.6.3 Text paging setup

Text pages can receive information including the point addresses of alarms, the alarm description, time of the alarm, and state (alarm or clear). The text pages may be viewed using a terminal such as Hyper-Terminal.

1. From the pa(G)ers menu (See figure 3.6), enter an ID number of the pager. Pager IDs are used in the alarm provisioning screen to designate the primary and secondary person/device being paged.
2. Enter type “T” for text paging under the “Type” heading.
3. Enter the phone number of the text paging device under the “Phone/Domain” heading.
4. Set the pager data rate (i.e. 300, 1,200, 2,400 or 9,600). The default baud is 1,200.
5. Select a pager word format (i.e. Data bits: 7 or 8, Parity: none (N), even (E) or odd (O), and Stop Bits: 1). The default setting is 7,E,1.

3.6.4 T/MonXM paging setup

T/MonXM can receive alarm information from the Net Guardian via dial-up and can display alarm information including the site number, alarm description, and threshold status.

1. From the pa(G)ers menu (See figure 3.6), enter an ID number of the pager. Pager IDs are used in the alarm provisioning screen to designate the primary and secondary person/device being paged.
2. Enter type “M” for T/MonXM paging under the “Type” heading.
3. Enter the phone number of the T/MonXM pager under the “Phone/Domain” heading.
4. Set the pager data rate (i.e. 300, 1,200, 2,400 or 9,600). The default baud is 1,200.
5. Select a pager word format (i.e. Data bits: 7 or 8, Parity: none (N), even (E) or odd (O), and Stop Bits: 1). The default setting is 7,E,1.

3.6.5 E-mail paging setup

The e-mail pager provides alarm notification via e-mail, with a description similar to that of the alpha-numeric pager.

1. From the pa(G)ers menu (See figure 3.6), enter an ID number of the pager. Pager IDs are used in the alarm provisioning screen to designate the primary and secondary person/device being paged.
2. Enter type “E” for e-mail paging under the “Type” heading.
3. Enter the domain name of the e-mail address under the “Phone/Domain” heading. This is the portion of an e-mail address *after*

the “@” symbol in name@domain.com. (There cannot be any spaces in the domain name)

4. Enter the e-mail recipient’s user name under the “PIN/Rcpt/Port” heading. This is the portion of an e-mail address *before* the “@” symbol in the name@domain.com. (There cannot be any spaces in the domain name)
5. Enter the IPA address of the mail server for SMTP e-mail pager types.
6. Exit the pa(G)ers menu and select the E)dit - s(Y)stem menu (See figure 3.2). Here you will set up the “from” address sent in e-mail messages sent from the Net Guardian. The “from” address is formatted using the “name” and “location” fields from the s(Y)stem menu as follows: name@location. Most e-mail programs can be set to perform a certain action if a message is received from a specified address, such as moving the message to a special “alarms” folder. Use the address entered here for such purposes.
7. Under the “Name:” heading, enter a descriptive name to identify the Net Guardian in e-mail messages. (There cannot be any spaces in the designated name)
8. Under the “Location:” heading, enter the domain of the Net Guardian. (There cannot be any spaces in the location name)

3.6.6 SNMP paging setup

The SNMP paging feature allows you to view alarm status from multiple SNMP Managers in addition to the main one, which is setup from the Ethernet Ports menu, that all alarms are reported to.

1. From the pa(G)ers menu (See figure 3.6), enter an ID number of the pager. Pager IDs are used in the alarm provisioning screen to designate the primary and secondary person/device being paged.
2. Enter type “S” for SNMP paging under the “Type” heading.
3. Set the SNMP port under the “PIN/Rcpt/Port” heading.
4. Enter the IP address of the computer to receive the SNMP traps.

3.6.7 TCP paging setup

The Net Guardian offers alarm status notification via multiple TCP ports. When an alarm condition occurs, standard formatted alarm data will be sent to the specified TCP points for use by a higher level master.

1. From the pa(G)ers menu (See figure 3.6), enter an ID number of the pager. Pager IDs are used in the alarm provisioning screen to designate the primary and secondary person/device being paged.
2. Select type “TCP” for text paging under the “TCP” heading.
3. Set the Pin/Rcpt/Port field to the TCP port number where alarm messages will be sent (from 1 to 65,536). Multiple ports can be defined by defining multiple pager IDs as TCP pagers and then entering the desired ports.
4. The TCP message can be viewed via a Telnet session. See figure 3.6.7 for an example message and table 3.6.7 for TCP message format information.

```
<MSG_BEG 00001>
VID : DPS Telecom
FID : NetGuardian SNMP v2.0C.0075
SITE: Yale Office
PNT : 99.01.01.01
DESC: RECTIFIER 1
STAT: CLEAR
DATE: 01/01/2001
TIME: 12:17:02
<MSG_END 00001>
```

Fig. 3.6.7 - Example TCP message.

Tbl. 3.6.7 - TCP alarm message field descriptions.

Heading	Description
MSG_BEG MSG_END	Sequential message number (e.g. 00001, 00002, etc.).
VID	Vendor ID.
FID	Net Guardian Firmware ID.
SITE	Net Guardian system name.
PNT	Point ID (port.address.display.point) - See Appendix A
DESC	Description set forth in the Alarm parameters.
STAT	Status of the alarm (Clear or Alarm).
DATE	Date the alarm occurred.
TIME	Time the alarm occurred.

3.7 Configuring Base Discrete Alarms

Choosing Alarm from the Edit menu takes you to the first page of the Alarm Configuration screen. All 32 discrete alarm points can be configured using this menu. Description of the alarm point; Polarity (nrm/rev); whether to use an SNMP Trap or not; and the primary/secondary pager used to report the alarm are configured in this submenu. All of the discrete alarms can be configured in this section of the editor using the choices shown in Table 3.7.

s(Y)stem L)ogin P)orts pa(G)ers A)larms R)elays					
a(N)alog s p(I)ng info T)imers D)ate/time n(V)ram (ESC) ? A					
ID	Description	Pol	SNMP Trap	Pager Pri	Sec
1	FIRE_SMOKE ALARM	Nrm	Y	3	4
2	DOOR ALARM	Nrm	N	3	1
3	EQUIPMENT ROOM TEMP	Nrm	Y	3	4
4	UPS ROOM 1 TEMP	Nrm	Y	3	4
5	UPS ROOM 2 TEMP	Nrm	Y	3	4
6	BATTERY ROOM TEMP	Nrm	Y	3	4
7	HPA DUCT AIRFLOW ALM	Nrm	N	1	2
8	COMMERCIAL POWER OUT	Rvs	Y	2	4
9	UTILITY GENERATOR SU	Nrm	Y	0	0
10	UPS GENERATOR SUM	Nrm	N	0	0
11	UTILITY GNRTR RUNNIN	Rvs	Y	1	2
12	UPS GNRTR RUNNING	Rvs	Y	1	2
13	UTILITY GNRTR RUNNING	Nrm	N	3	2
14	UPS GNRTR ONLINE	Rvs	Y	3	2
15	DEHYDRATOR WG PRESSUR	Nrm	N	1	4
16	DEICER FUEL OVERFLOW	Nrm	N	1	2
Alarm ID (ESC exit, TAB next page) :_					

Fig. 3.7 - This screen allows you to edit the first 16 alarms.

Tbl. 3.7 - Alarm point definition fields.

Field	Description
ID	This shows 32 discrete input points where you set alarm activation conditions. (Non-editable field)
Description	Description of the 32 alarms.
Polarity	Polarity: Normal=Contact closure is an alarm. If Polarity is reversed, the alarm is clear when closed.
Trap	Trap toggles the SNMP information. Y=Send Trap N=Don't Sent Trap Allows you to designate if an SNMP trap is to be sent when an alarm condition exists. Additional traps can be sent by using primary and secondary pagers.
Primary and Secondary Pagers	Primary Pager and Secondary pager: Allows you to designate pagers. The Net Guardian 832A will issue one call to the primary (pager) device, followed by one call to the secondary (pager) device. Note: The Pager device can be an ASCII terminal, T/MonXM element manager or IAM element manager, E-mail, or multiple SNMP managers as well as an alpha or numeric pager. Enter IDs (1-8) from pager list.

3.8 Configuring the Controls (Relays)

The relays of the Net Guardian 832A can be identified and configured using the R)elays submenu. A description can be entered for each of the relays. You can also designate whether or not to send an SNMP Trap when a relay is actuated.

1. The ID field represents the ID number of the relay. Enter a description for each relay being used.
2. Choose whether or not to send an SNMP Trap (“Y” for yes and “N” for no). This allows you to designate if an SNMP trap is to be sent when a control point operates.

```

E)dit M)onitor P)ing S)tats R)eset modem (ESC) ? E

s(Y)stem L)ogin P)orts pa(G)ers A)larms R)elays
  a(N)alogs p(I)ng info T)imers D)ate/time n(V)ram (ESC) ? R

ID      Description              SNMP
1      START UPS GENERATOR      Y
2      STOP UPS GENERATOR       Y
3      START UTILITY GNRTR      Y
4      STOP UTILITY GNRTR       Y
5      LOCK COMP. RM DOOR       Y
6      UNLOCK COMP. RM DOOR     Y
7      GE2 DE-ICING TO AUT      Y
8      01.08 Power Out          Y

Relay ID: _

```

Fig. 3.8- The R)elays screen allows viewing and changing the relay parameter.

3.8.1 Echoing alarm points to relays

The Net Guardian allows the user to echo an alarm point state to activate a relay. Any of the Net Guardian’s discrete alarms, system alarms, ping alarms, or analog alarms may be echoed to activate a relay in the event an alarm is triggered. Follow the directions below to enable the echoing functionality.

1. In the R)elay description field, enter the display, alarm point, and description of the alarm you wish to echo. For example, if echoing discrete alarm 8, enter 01.08-*your alarm description* (the display and alarm point are formatted as “DD.PP” where DD=the display number and PP=the point number). See Appendix A for a complete list of display and point numbers.

Note: With the “echo” mode activated, the relay will only activate if the designated alarm is triggered. It can not be activated manually.

3.9 Setting the Analog Parameters

Each of the Net Guardian 832A's analog channels must be individually configured to monitor external analog data. The ADCs (analog to digital converters) support a range of -79.9 to +79.9 VDC. There are four alarm trip points (thresholds) in ascending order: major under, minor under, minor over, and major over. You can choose the values for each of the thresholds on all channels. As with the other alarms, you can designate whether or not to send an SNMP Trap when a threshold is crossed. The primary/secondary pager used to report the alarm is also set here. The thresholds must be set from Under to Over in either ascending or descending potential (or current) order. Thus the settings of 10, 5, -5 and -10 corresponding respectively to major under, minor under, minor over and major over is valid.

The analog alarms are set to measure voltage by default and the thresholds are reported as “native units”. For example, Channel 1 below is measuring room temperature. The voltage for that channel varies between 1 and 5 VDC, to be reported as degrees Fahrenheit (“native units”) where 1 volt represents 0 degrees Fahrenheit and 5 volts represents 95 degrees Fahrenheit.

To change any one analog alarm to measure current instead, a jumper setting must be changed. Refer to the PCB settings section (2.3.8) for details on jumper locations and positions. The jumper inserts a 250 ohm shunt resistor across the input to convert the sensors current output to volts. Use Ohms law to find the voltage drop across the 250 ohm shunt resistor (multiply the current by the resistance 250 ohms). Please refer to the operation manual for your sensor to determine any other conversion factors. This will allow you to correctly set the thresholds for over and under conditions.

Setting the Analog parameters

1. From the E)dit menu, select a(N)alogs.
2. Select the Analog Channel ID you wish to configure and press <Enter>. (See figure 3.9a)
3. Select D)escription and enter a description (i.e. Room Temperature, Relative Humidity, etc.) and press <Enter>. (See figure 3.9a)
4. Select U)nits.
5. Select U)nits again and enter a units reference corresponding to your native units (i.e. F for Fahrenheit, RH for Relative Humidity, etc.) and press <Enter>.

```

Analog Channel ID:  1

ID Description      Unit      Major      Minor      Minor      Major      SNMP      Pagers
 1                VDC      Under      Under      Over       Over       Trap      Pri  Sec
 1                VDC      -79.0000  -35.0000   35.0000    79.0000    Y         0   0

D)escription  U)nits  t(H)resholds  T)rap  P)ri.Pgr  S)ec.Pgr  (ESC)? D
Description:  ROOM TEMP

ID Description      Unit      Major      Minor      Minor      Major      SNMP      Pagers
 1 ROOM TEMP       VDC      Under      Under      Over       Over       Trap      Pri  Sec
 1 ROOM TEMP       VDC      -79.0000  -35.0000   35.0000    79.0000    Y         0   0

D)escription  U)nits  t(H)resholds  T)rap  P)ri.Pgr  S)ec.Pgr  (ESC)? U

          Reference 1          Reference 2
ID      VDC  =  VDC      VDC  =  VDC
1      -35.0000  -35.0000   35.0000   35.0000

U)nits  a)Ref 1 VDC  b) Ref 1 Units  c) Ref 2 VDC  d) Ref 2 Units (ESC)? U

```

Fig. 3.9a - The analog alarm inputs support a range of -79.9 to +79.9 VDC or 4-20mA.

6. Select a) Ref 1 VDC and enter the minimum output in volts DC of the analog device being configured* and press <Enter>. (See figure 3.9b)
 7. Select b) Ref 1 Units and enter the native units that correspond to the minimum output entered in the previous step and press <Enter>.
 8. Select c) Ref 2 VDC and enter the maximum output in volts DC of the analog device being configured* and press <Enter>. (See figure 3.9b)
 9. Select d) Ref 2 Units and enter the native units that correspond to the minimum output entered in the previous step and press <Enter>. **
 10. Once the Reference units are set, press escape to return to the previous menu where the t(H)reshold settings can be configured.
- * *The Net Guardian performs the scaling calculations automatically.*
- ** *A number different than your native unit amount may appear. Change these figures in the t(H)reshold menu.*

```

U)nits  a)Ref 1 VDC  b) Ref 1 Units  c) Ref 2 VDC  d) Ref 2 Units (ESC)? A

Reference 1 VDC: 1

      Reference 1              Reference 2
ID   VDC   =   F              VDC   =   F
1    1.0000  0.0000          5.0000   95.0000

U)nits  a)Ref 1 VDC  b) Ref 1 Units  c) Ref 2 VDC  d) Ref 2 Units (ESC)? B

Reference 1 Units:  0

      Reference 1              Reference 2
ID   VDC   =   F              VDC   =   F
1    1.0000  0.0000          5.0000   95.0000

U)nits  a)Ref 1 VDC  b) Ref 1 Units  c) Ref 2 VDC  d) Ref 2 Units (ESC)? C

```

Fig. 3.9b - Enter the Reference 1 VDC and native unit settings.

11. Select the t(H)resholds menu. (See figure 3.9c)
12. Set the major and minor threshold figures (i.e. 0, 15, 85 and 95) and press (ESC) after all thresholds are entered. (See figure 3.9c)
13. Repeat steps 1 through 11 for each analog parameter being configured.

ID	Description	Unit	Major Under	Minor Under	Minor Over	Major Over	SNMP Trap	Pagers Pri	Pagers Sec
1	ROOM TEMP	VDC	-79.0000	-35.0000	35.0000	79.0000	Y	0	0

```

D)escription  U)nits  t(H)resholds  T)rap  P)ri.Pgr  S)ec.Pgr (ESC)? H

Major under:  -0.0017
Minor under:   14.9990
Minor over:    89.9982
Major over:    95.0000

A) Major under  B) Minor under  C) Minor over  D) Major over  (ESC)? A

Threshold value:  0

A) Major under  B) Minor under  C) Minor over  D) Major over  (ESC)? B

Threshold value:  15

```

Fig. 3.9c - Enter the desired thresholds for each analog channel.

3.10 Configuring Ping Targets

The Net Guardian can ping up to 32 network elements. The 32-target ping table can be viewed and changed under the P(I)ng menu selection. Each of the ping targets can be provisioned with a description, an IP address, a choice to use SNMP Traps, and primary/secondary pager numbers.

```
s(Y)stem L)ogin P)orts pa(G)ers A)larms R)elays
a(N)alog p(I)ng info T)imers D)ate/time n(V)ram (ESC) ? I
```

			SNMP .Pager.		
ID	Description	IP Address	Pri	Sec	
1	Switch	126.010.220.155	N	0	0
2	Router TX1	126.010.220.150	N	0	0
3	Server LAX49A	126.010.220.149	N	0	0
4	Net Element	126.010.220.148	N	0	0
5	NOC primary	126.010.220.130	N	0	0
6	NOC secondary	126.010.220.131	N	0	0
7	OPS PC #1	126.010.220.132	N	0	0
8	OPS PC #2	126.010.220.133	N	0	0
9		255.255.255.255	N	0	0
10		255.255.255.255	N	0	0
11		255.255.255.255	N	0	0
12		255.255.255.255	N	0	0
13		255.255.255.255	N	0	0
14		255.255.255.255	N	0	0
15		255.255.255.255	N	0	0
16		255.255.255.255	N	0	0

Ping ID (ESC exit, TAB next page):

Fig. 3.10 - The p(I)ng Info submenu allows you to change ping targets.

Tbl. 3.10 - Ping target field descriptions.

Field	Description
ID	Fixed number designating the line number in the list of devices to be pinged.
Description	Description of the device to be pinged.
IP Address	Address of the device to be pinged.
SNMP Trap	Trap toggles the SNMP information. Y= Send N=Don't Send Allows you to designate if an SNMP trap is to be sent when an alarm condition exists.
Pager, Primary	Pager ID for first pager to be called in case of an alarm condition.
Pager, Secondary	Pager ID for second pager to be called in case of an alarm condition (in case the primary pager does not acknowledge).
Ping	Repeatedly pings the device for status. OK= device responding. NOK_(error code) = device not responding. Error codes are listed in Table K.

3.11 Setting System Timers

The system timers allow you to control the rate of your ping activity. Ping timer settings allow you to balance network traffic against alarm response times. Though you can change the values from their default settings, it is recommended that you use either the default settings or plan your settings so that there is no conflict among the timers. Specifically, the FAIL time should be set to several times the CYCLE time to allow multiple PINGs before a FAIL is declared. Likewise, the CYCLE time should be set to several times the TRY time.

Note: *The smaller the CYCLE number, the sooner you will find out about failures, but you will also increase traffic on your LAN.*

```
s(Y)stem L)ogin P)orts pa(G)ers A)larms R)elays
a(N)alogs p(I)ng info T)imers D)ate/time n(V)ram (ESC) ? T

Cycle      :    0 sec
Wait       :    0 sec
Fail       :    0 sec
Sound      :    0 sec
Channel    :    2 min
Craft      :   10 min
Debounce   :   600 msec

C)ycle W)ait F)ail S)ound c(H)annel d(E)bounce (ESC) ?
```

Fig. 3.11a - The *T)imers* submenu gives access to the system timers.

Tbl. 3.11 - *Timer Settings.*

Field	Description
Cycle	How often the Net Guardian will go through its list of ping targets and attempts to reach them with an ICMP ping. Set P)eriod (0 to 120) and U)nits (toggles between minutes and seconds). Default= 60 seconds. Total range is 0-120 minutes.
Try	The Net Guardian waits after sending a ping request before it determines that the target is unreachable. Set P)eriod (0-120) and U)nits (toggles between minutes and seconds). Default = 8 seconds. Total range is 0-120 seconds or 0-120 minutes. (Busy networks might necessitate a longer wait time here).
Fail	Period of time over which, if a unit has not responded, it is considered failed. Set P)eriod (0 to 120) and U)nits (toggles between minutes and seconds). Default = 5 minutes. Total range is 0-120 seconds or 0-120 minutes.
Sound	Sets how long the speaker sounds an alarm condition. P)eriod = number of units from 0 to 120. U)nits = toggles units in sec or min.
Channel	Determines the period of time over which, if there is no activity on any of the data ports designated as channel ports (see section 3.5.5), it is considered failed. Set between 0 and 120 (min or sec). Alarm activity is indicated in Display 11, Point 62 (See Appendix A - Display Mapping).
Craft	Determines the period of time over which, if the device connected through a port designated as a “craft” port doesn’t reset the craft timer, an alarm will be triggered. The connected device should be configured to navigate through the text menus to reset the craft timer. If the device fails to reset the craft timer, an alarm condition will occur at display 11, point 63. Set between 0 and 120 (min or sec). Zero disengages the timer function. Alarm activity is indicated in Display 11, Point 63 (See Appendix A - Display Mapping).
Debounce	Determines the amount of time before discrete alarms are triggered (between 3 and 1000 msec).

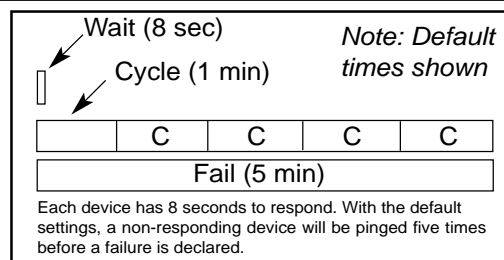


Fig. 3.11b - When a target fails to respond to a ping within the fail time period, a fault is declared.

3.12 Setting the System Date and Time

The date is entered in the mm/dd/yyyy format and the time is entered in the hh:mm:ss format. The date and time can also be set from an SNMP manager.

Note: *The date and time will need resetting following a power failure unless your Net Guardian is equipped with the real-time clock option.*

```
E)dit  M)onitor  P)ing  S)tats  R)eset modem (ESC) ? E

s(Y)stem  L)ogin  P)orts  pa(G)ers  A)larms  R)elays
  a(N)alog  p(I)ng info  T)imers  D)ate/time  n(V)ram (ESC) ? D

Date :   06-11-2001
Time :   06:36:54

D)ate  T)ime (ESC) ?
```

Fig. 3.12 - Viewing and changing the date and time.

3.13 Saving Changes or Resetting Factory Defaults

Your Net Guardian 832A comes equipped with Non Volatile (NV) RAM which enables the retention of data in the event of power loss. This section of the editor allows you to V)erify, W)rite, and R)eload the n(v)ram.

- Pressing the 'V' key causes the Net Guardian 832A to verify the NVRAM status.
- Pressing the 'W' key causes the current data in RAM to be written to NVRAM and then verified. A result code of "complete" means that the write was successful.
- Press the 'R' key to reload factory defaults into NVRAM. DO NOT SELECT THIS OPTION UNLESS YOU WANT TO REENTER ALL OF YOUR CONFIGURATION INFORMATION AGAIN.

```
E)dit  M)onitor  P)ing  S)tats  R)eset modem (ESC) ? E

s(Y)stem  L)ogin  P)orts  pa(G)ers  A)larms  R)elays
  a(N)alog  p(I)ng info  T)imers  D)ate/time  n(V)ram (ESC) ? V

V)erify  W)rite  R)eload (ESC) ? W

Write.....Verify.....complete!
```

Fig. 3.13 - Write to the n(V)ram to save changes made to the Net Guardian 832A.

3.14 PPP Net Guardian

The PPP (point to point protocol) version of the Net Guardian allows the Net Guardian to dial into the LAN via a POTS line instead of through the ethernet port. This version is intended for remote sites that are off network -- sites where there is only a standard POTS line but no ethernet connection available. The Net Guardian can gain access to the LAN by dialing into the network in the same way that a workstation dials into an ISP. Because the modem is used to establish a constant network connection, however, features such as alpha and numeric paging are not available with the PPP version.

Connect a PC running terminal emulation software to the craft port on the front of the Net Guardian 832A using a DB9 download cable (provided) (See figure 3 on page 18). Set your serial port to match the data rate and word format currently defined for the Net Guardian 832A (factory default is 9600 N, 8, 1). Also in your terminal emulation software, set the Flow control to "None." When a connection is established (sometimes accompanied by receipt of a hex byte), type DPSCFG <Enter> to activate the configuration menu.

Note: When configuring the Ethernet port information in the PPP version of the Net Guardian, the Unit Address, Subnet Mask, and Default Gateway are uneditable fields because point to point protocol is used.

1. Enter your password (factory default is dpstelecom).
2. Select C)onfig.
3. Select E)dit.
4. Select P)orts.
5. Select P)PP.
6. Enter a username, password and the phone number that the Net Guardian will use to dial into your network.
7. Selecting C)ompression toggles the use of TCP header compression. (Y = yes and N = no).

```
*****
Password: *****

NetGuardian v2.0A.0493
C)onfig  P)roxy  D)ebug  e(X)it

E)dit  M)onitor  P)ing  S)tats  R)eset modem (ESC) ? E

s(Y)stem  L)ogin  P)orts  pa(G)ers  A)larms  R)elays
  a(N)alogs  p(I)ng info  T)imers  D)ate/time  n(V)ram (ESC) ? P

E)thernet  M)odem  C)raft  D)ata  P)PP  O)ptions (ESC) ? P

Username      :
Password      :
Phone         :
Compression   :    Y

U)sername  P)assword  p(H)one  C)ompression (ESC) ?
```

Fig. 3.14 - The PPP version of the Net Guardian offers access to the LAN via a standard telephone line.

3.15 DCPx Net Guardian

The DCPx firmware version of the Net Guardian performs all of the functions of the SNMP Net Guardian with the exception of sending SNMP traps. It is used when an IAM or T/MonXM is the upper level master instead of an SNMP Manager. In each of the software provisioning screens (including the web browser), the SNMP trap field has been eliminated. However, in the "System" menu of the DCPx firmware version, a "Unit ID" field is included to identify the address of the Master unit that the Net Guardian is reporting to. The firmware version loaded on your Net Guardian is indicated on the LCD.

Monitoring

Chapter 4

4.1 Monitoring the Net Guardian 832A

Connect a PC running VT-100 terminal emulation software to the craft port or connect, via LAN using a TELNET client (with VT-100 emulation) to port 2002 to reach the M)onitor menu selection. This section allows you to do full-system monitoring for your Net Guardian 832A which includes all alarms, ping information, relays, analogs, and system status.

```

Password: *****

NetGuardian 832A v1.0A.0135
C)onfig P)roxy D)ebug e(X)it

E)dit M)onitor P)ing S)tats R)eset modem (ESC) ? M

A)larms P)ing Info R)elays a(N)alog S)ystem (ESC) ?

```

Fig. 4.1 - The monitor menu allows status checking on all elements.

4.1.1 Monitoring Base Alarms

The A)larm choice of the M)onitor menu allows you to view the status of the device connected to the discrete input. Under the “Status” heading, the word “Alarm” will appear if an alarm has been activated and the word “Clear” will appear if an alarm condition is not present.

```

16 DEICER FUEL OVERFLOW Clear
ESC to exit Any key to continue
ID   Description           Status
17   GNRTR FUEL OVERFLOW   Clear
18   UPS SUMMARY ALARM     Clear
19   AIR COND. SUMMARY     Clear
20   ICY CONDITION         Clear
21   C5 DE-ICING SYS ON    Alarm
22   C5 ANTENNA UP TO TEM   Clear
23   GE2 DE-ICING SYS AUT   Clear
24   GE2 DE-ICING SYS MAN   Clear
25   GE2 DE-ICING SYS ON    Clear
26   GE2 DE-ICER 1 ON      Alarm
27   GE2 DE-ICER 2 ON      Alarm
28   GE2 DE-ICER 3 ON      Alarm
29   GE2 DE-ICER 4 ON      Alarm
30   30                     Clear
31   31                     Clear
32   32                     Clear
ESC to exit Any key to continue

A)larms P)ing Info R)elays a(N)alog S)ystem (ESC) ? _

```

Fig. 4.1.1 - This example shows page two of the discrete alarms.

4.1.2 Monitoring Ping Targets

The Ping Info choice of the M)onitor section displays the status of all your ping targets. Under the “Status” heading, the word “Alarm” will appear if an alarm has been activated and the word “Clear” will appear if an alarm condition is not present.

```

16                255.255.255.255  Clear
ESC to exit  Any key to continue

ID   Description      IP Address      Status
17   Switch           126.010.210.037 Clear
18   Router TX1       126.010.210.038 Clear
19   Server LAX49A    126.010.210.039 Clear
20   Net Element      126.010.210.040 Clear
21   NOC primary      126.010.210.041 Clear
22   NOC secondary    126.010.210.042 Clear
23   OPS PC #1        126.010.210.043 Clear
24   OPS PC #2        126.010.210.044 Clear
25   025              126.010.210.045 Clear
26   026              126.010.210.046 Clear
27   027              126.010.210.047 Clear
28   028              126.010.210.048 Clear
29   029              126.010.210.049 Clear
30   030              126.010.210.050 Clear
31   031              126.010.210.051 Clear
32   032              126.010.210.052 Clear

A)larms P)ing Info R)elays a(N)alog S)ystem (ESC)? _

```

Fig. 4.1.2 - The P)ing info submenu allows you to change ping targets.

4.1.3 Monitoring and Operating Relays (Controls)

Your Net Guardian 832A comes equipped with 8 relays which can be used to control external devices. The M)onitor, R)elays menu allows you to monitor the status of your relays. The Net Guardian’s 8 relays are set to N.O. as the factory default, but each or all of them can be changed to N.C. by changing their respective jumper (Refer to the PCB settings section 2.3.8 for jumper locations and positions).

1. To operate a relay, use the O)pr command and then select the relay ID number you wish to operate. To release an operated relay, use the R)ls command. Then, select the relay ID number you wish to release.
2. Select the M)om command to momentarily actuate a relay.

```

E)dit M)onitor P)ing R)eset modem (ESC)? M

A)larms P)ing Info )Relays a(N)alog S)ystem (ESC)? R

ID   Description      Status
1    START UPS GENERATOR  Rls
2    STOP UPS GENERATOR   Rls
3    START UTILITY GNRTR  Rls
4    STOP UTILITY GNRTR   Rls
5    LOCK COMP. RM DOOR   Rls
6    UNLOCK COMP. RM DOOR Rls
7    GE2 DE-ICING TO AUT  Rls
8    GE2 DE-ICING OFF     Rls

S)tatus      O)pr R)ls M)om (ESC)? _

```

Fig. 4.1.3 - The eight relays can be operated from this screen.

4.1.4 Monitoring Analogs

This screen will show you the descriptions that you have previously entered for your 8 analogs, the current reading, and the alarm status. The value shown is a “snapshot” of the channels measurement, not a real-time reading. Therefore, each adjustment should be followed by the a(N)alog menu choice to refresh the readings. Alarm status indicates that a preset threshold has been crossed (designated by an “x”).

The eight analog measuring inputs, as mentioned previously, are set to measure voltage as the factory default. If your sensors output is current, you will need to change the appropriate analog jumpers, as described in the PCB settings section, to the current measuring position. The scaling worksheet in the provisioning section converts all readings shown here into “native” units such as degrees Celsius or percent relative humidity.

```
E)dit M)onitor P)ing S)tats R)eset modem (ESC)? M

A)larms P)ing info R)elays a(N)alog S)ystem (ESC)? N
```

Chn	Description	Reading	MjU	MnU	MnO	MjO	Err
1	BATTERY A	0.0000	-	-	-	-	-
2	BATTERY B	0.0000	-	-	-	-	-
3	COMP. ROOM TEM	79.231 F	-	-	-	-	-
4	INSIDE TEMPERA	81.136 F	-	-	-	-	-
5	OUTSIDE TEMPER	93.126 F	-	-	x	-	-
6	BATTERY RM TEM	85.594 F	-	-	-	-	-
7	RELATIVE HUMID	49.168 %	-	-	-	-	-
8	AN 8	0.0000	-	-	-	-	-

```
A)larms P)ing Info R)elays a(N)alog S)ystem (ESC)? _
```

Fig. 4.1.4 - This display allows you to monitor your eight analog inputs.

4.1.5 Monitoring System Alarms

System alarms are identified and displayed via the M)onitor/S)ystem menu choice. The following screen is a list of System alarms. A complete table of System alarms appearing on display 11 is given in Appendix A. Under the “Status” heading, the word “Alarm” will appear if an alarm has been activated and the word “Clear” will appear if an alarm condition is not present.

```
A)larms P)ing Info R)elays a(N)alog S)ystem (ESC)? S
```

ID	Description	Status
33	Power Up	Alarm
36	Lost Provisioning	Clear
38	LAN not active	Alarm
41	Modem not responding	Clear
42	No Dial-tone	Clear
43	SNMP trap not sent	Alarm
44	Pager Que Overflow	Clear
45	Notification failed	Clear
46	Craft RcvQ Full	Clear
47	Modem RcvQ Full	Clear
48	Data 1 RcvQ Full	Clear
49	Data 2 RcvQ Full	Clear
50	Data 3 RcvQ Full	Clear
51	Data 4 RcvQ Full	Clear
52	Data 5 RcvQ Full	Clear
53	Data 6 RcvQ Full	Clear
54	Data 7 RcvQ Full	Clear
55	Data 8 RcvQ Full	Clear

```
A)larms P)ing Info R)elays a(N)alog S)ystem (ESC)? _
```

Fig. 4.1.5 - System alarms can be viewed from the M)onitor, S)ystem submenu.

4.1.6 Monitoring Data Port Activity

This selection provides the status of the eight data ports by providing an ASCII description under “Port Transmit” and “Port Receive” (refer to section 3.4.5 for data port settings). See Appendix C - ASCII Conversion, for specific ASCII symbol conversion.

```

A)larms  P)ing Info  R)elays  a(N)alog  S)ystem  p(O)rts (ESC) ? 0

Data Port ID (1-8): 1

a)Transmit  b)Receive (ESC) ? A

Port 1 Transmit (ESC) : <--

a)Transmit  b)Receive (ESC) ? B

Port 1 Receive (ESC) : <--

a)Transmit  b)Receive (ESC) ? <--

A)larms  P)ing Info  R)elays  a(N)alog  S)ystem  p(O)rts (ESC) ? <--

```

Fig. 4.1.6a - Data port activity can be viewed from the M)onitor, p(O)rts submenu.

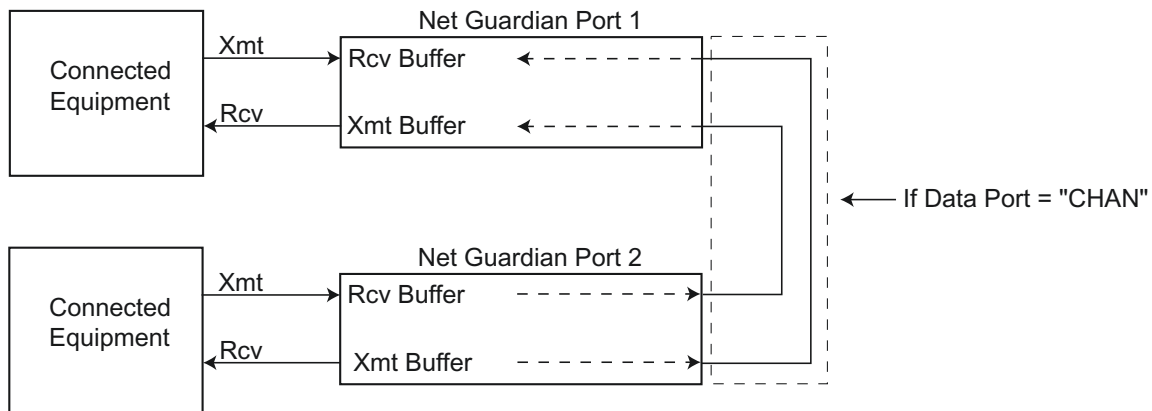


Fig. 4.1.6b - To view the data transmitting from the connected equipment, select the receive queue from the Net Guardian. To view the data being received by the connected equipment, select the transmit queue from the Net Guardian.

4.2 Viewing Live Target Pings

Any of the 32 pre-defined IP addresses can be “pinged” using this menu choice. Inputting the IP address ID number (1-32) (See section 3.9) causes the Net Guardian to ping that address in real time until you hit <Esc>.

```

Password: *****

NetGuardian 832A v1.0A.0135
C)onfig P)roxy D)ebug e(X)it

E)dit M)onitor P)ing S)tats R)eset modem (ESC) ? P

Ping Address / ID (1-32) : 1

Pinging 126.10.220.198 - press ESC to stop....OK.OK.OK.OK

```

Fig. 4.2 - You can watch the Net Guardian continuously ping an IP address that has been defined in the Ping table.

4.3 Viewing your System Statistics

Various statistics about the system and its operation are available under the S)tats menu. The number of successful pages is one of the more important statistics available, since it can be used to determine the effectiveness of the reporting method and pathway.

```

E)dit M)onitor P)ing S)tats R)eset modem (ESC) ? S

Product: NetGuardian 832A
Version: v1.0A
  Build: 0135
  Loader: v1.1a
  Booter: v1.0D
Uptime: 8203 hours, 50 minutes, 55 seconds
Statistics-

```

Action	Attempts	Failures	Retries
SNMP Traps	624	0	84
Alpha pages	254	0	N/A
Numeric pages	109	0	N/A
TMon pages	824	0	N/A
Text pages	0	0	N/A
Email pages	413	0	N/A

Fig. 4.3 - The Stats menu gives system information and statistics.

4.4 Proxy menu

Proxy connections can take place to reach-through to the craft port, modem port or any of the other 8 serial ports. This can be done to allow you to monitor and/or control additional devices via your connection to the Net Guardian 832A. Data presented and “hand-shaking” will be as specified by the connected device.

To cancel the proxy connection, wait a 1/2 second and then type the following within a 1 second time period: @@@ <Enter>

```
NetGuardian 832A v1.0A.0135
C)onfig P)roxy D)ebug e(X)it

Proxy to: L)ist M)odem 1 2 3 4 5 6 7 8 <ESC> L

Available Data Ports:
1) ASCII Device
2) DCP Device
3) Monitor RS232
4) Monitor RS232
5) DDM2000
6) Router 1
7) NG Expansion
8) GLD

Proxy to: L)ist M)odem 1 2 3 4 5 6 7 8 <ESC> 1

Proxy Established
```

Fig. 4.4 - Access devices connected to the 7 DCE type data ports on the back panel through the P)roxy menu selection.

4.5 LCD Menu Operation

Controlling Display Speed

The scroll speed can be temporarily increased by pressing and holding the '+' key while the message is active.

Standard Prompt

At the beginning of the sequence, the standard prompt, "Press MENU for front panel options" will appear, followed by a display of the firmware version.

Standing Alarms

"Discrete Alarms:" will appear on the scrolling text when there are standing alarms. This will be followed by the alphanumeric description that the user has entered for each alarm that is standing.

Latched Controls

If there are latched relays, one section of the scrolling message will start with the message, "Relays:" and will be followed by an alphanumeric description entered by the user for each latched relay.

Ping Alarms

The Ping Alarms section is designed for any targets the user has entered that have become unreachable within the timing dynamic that has been provisioned or is currently active. A section of the scrolling text will state, "Ping Alarms:", which will be followed by the alphanumeric description the user has entered for the unreachable ping target.

Analog Channels

This section of the scrolling messages will begin with, "Analog:" and followed by an entry for each channel. An active analog channel is a channel with a threshold condition. The channel entry contains an alphanumeric description of the channel (as entered by the user) and the voltage readout of the channel last read. Finally, a single character will represent the highest standing alarm derived from the reading. A lowercase 'o' represents a minor over; an uppercase 'O' represents a major over; a lowercase 'u' for a minor under; and an uppercase 'U' for a major under.



Fig. 4.5 - Start of 2-line, scrolling LCD sequence.

4.5.1 Sounds from the Net Guardian 832A

The LCD menu option "Sound off" will suppress all sounds for a 10-, 20- or 30-minute period. Select '0' to cancel the suppression. The alarm will sound for the configured number of seconds (config/edit/timers/sound menu) (See section 3.10). The Net Guardian 832A will emit a sound when there is an Ethernet link failure caused by unplugging the LAN cable and when an alarm is active. An Ethernet failure will emit a hi-lo or warbling tone and a reportable alarm will emit an intermittent beep. An alarm sound can be turned off by pressing any front panel button. Any reporting alarm sound will continue to its normal end even when a subsequent alarm is detected. Stopping the sound by pressing a front panel button allows the next alarm, if any, to sound.

4.5.2 Reboot and Forced Configuration

The LCD menu gives two other options:

- Reboot: The same as selecting the reset option in the configuration menu.
- Run Config: Forces the configurator to run on the craft port at 9600, N, 8, 1.

4.6 Front Panel LED Operation

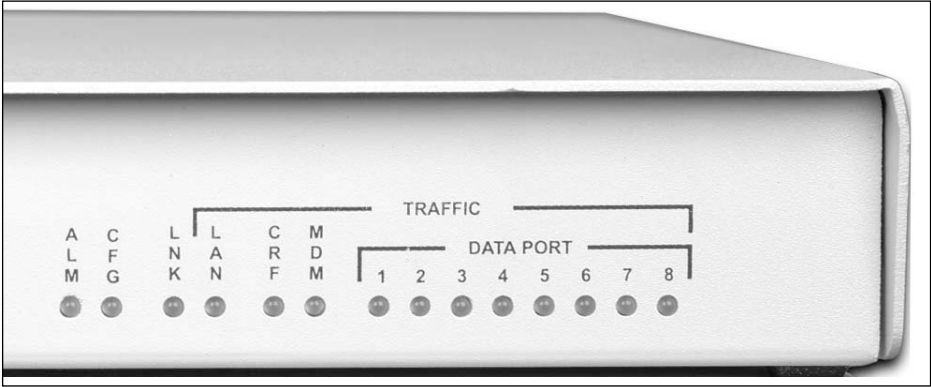


Fig. 4.6 - Net Guardian 832A's LEDs give at-a-glance status indication.

Tbl. 4.6 - LED Indications.

LED	STATUS	DESCRIPTION
ALM	Flashing Red	New alarm status
	Solid Red	New alarm acknowledged, condition still present
CFG	Flashing Red	Net Guardian configuration information not verified (re-configuration needed)
	Flashing Green	Net Guardian configuration information verified, system operational
LNK	Green	Ethernet link OK
	Red	Ethernet link failure
LAN, CRF, MDM, DATA 1-8	Flashing Green	Data transmit
	Flashing Red	Data receive

4.7 Component Review

Net Guardian 832A's alarm inputs accept any contact closure or opening type of event notification, such as door switches, fuse alarms, major and minor equipment alarms, high temperature alarms and tower light monitors. The unit provides 8 control relay outputs for operating standby equipment, door locks or emergency lighting. In addition, there are 8 analog inputs with an input range of -79.9 to +79.9VDC or 4-20mA. The following is an overview of the components of the Net Guardian 832A.

Craft port

The craft port can be connected to the COM port of a computer to locally configure the Net Guardian 832A using any standard terminal emulation software (e.g. HyperTerm, Xtalk, etc.). You can also connect via proxy to any of the data ports or the modem.

10BaseT Port

The 10BaseT port is used to connect to your Ethernet LAN. This connection is used to “ping” up to 32 other devices to determine their operational status. If a given device does not respond, it is reported as off line. This port can also be used to configure the Net Guardian 832A, view alarms and access other devices connected to the reach through ports.

Modem port

The modem port is a modem interface to a telephone line. The modem operates at 1200, 2400, 9600 and Auto Baud options. When the Net Guardian 832A has an event to report, it can use this port to dial out to a paging terminal in addition to reporting via SNMP. This port may also be used to configure the Net Guardian 832A.

8 reach-through ports

The 8 reach-through ports can be connected to any device with an RS232 interface. The Net Guardian 832A provides a “reach through proxy” to any one of these ports. This proxy function is available via all methods of connecting to the Net Guardian 832A including modem and TELNET connections. Devices with only a serial communication port can be transferred to the LAN, utilizing it's benefits and flexibility using the reach through ports. Data sent to the RS232 serial ports is transferred to a “proxy” port at the Net Guardian's IP address. If the Net Guardian is reporting to T/MonXM or an IAM, the data ports can act as essentially 8 additional ports for polling DCP devices or ASCII devices.

Display Mapping

Appendix A

Tbl. A1- Display descriptions and SNMP Trap numbers for the Net Guardian.

Port	Address	Display	Description	SNMP Trap #s *	
				Set	Clear
99	1	1	Discrete Alarms 1-32	8000-8031	9000-9031
99	1	2	Ping Table	8064-8095	9064-9095
99	1	3	Analog Channel 1**	8128-8131	9128-9131
99	1	4	Analog Channel 2**	8192-8195	9192-9195
99	1	5	Analog Channel 3**	8256-8259	9256-9259
99	1	6	Analog Channel 4**	8320-8323	9320-9323
99	1	7	Analog Channel 5**	8384-8387	9384-9387
99	1	8	Analog Channel 6**	8448-8451	9448-9451
99	1	9	Analog Channel 7**	8512-8515	9512-9515
99	1	10	Analog Channel 8**	8576-8579	9576-9579
99	1	11	Relays/System alarms (See table below)	8640-8673	9640-9673

* The TRAP number ranges shown correspond to the point range of each display. For example, the SNMP Trap “Set” number for alarm 1 (in Display 1) is 8000, “Set” for alarm 2 is 8001, “Set” for alarm 3 is 8002, etc.

** The TRAP number descriptions for the Analog channels (1-8) are in the following order: minor under, minor over, major under, and major over. For example, for Analog channel 1, the “Set” number for minor under is 8128, minor over is 8129, major under is 8130, and major over is 8131.

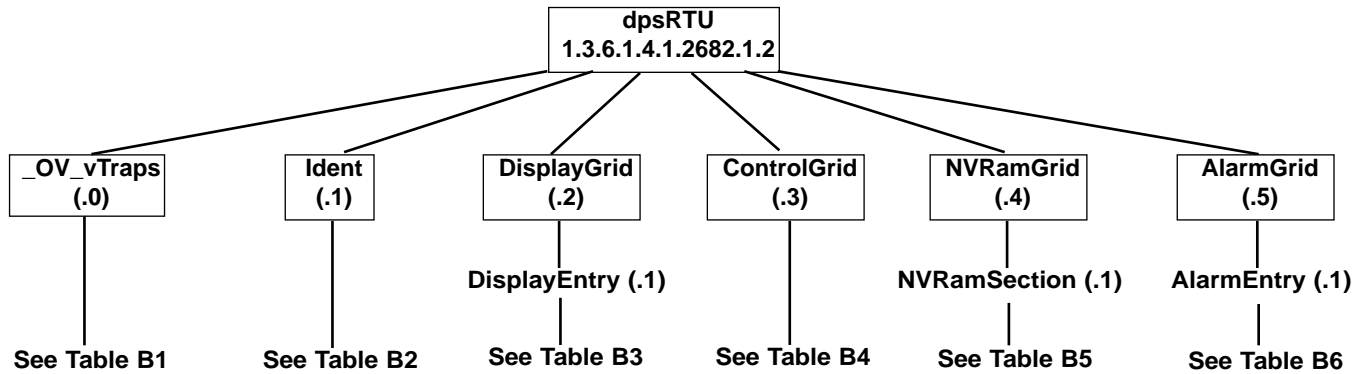
Tbl. A2 - Display 11 (System alarms) point descriptions.

Points	Description	SNMP Trap #s		Points	Description	SNMP Trap #s	
		Set	Clear			Set	Clear
1	Relays	8640	9640	47	Modem RcvQ full	8657	9657
2	Relays	8641	9641	48	Serial 1 RcvQ full	8658	9658
3	Relays	8642	9642	49	Serial 2 RcvQ full	8659	9659
4	Relays	8643	9643	50	Serial 3 RcvQ full	8660	9660
5	Relays	8644	9644	51	Serial 4 RcvQ full	8661	9661
6	Relays	8645	9645	52	Serial 5 RcvQ full	8662	9662
7	Relays	8646	9646	53	Serial 6 RcvQ full	8663	9663
8	Relays	8647	9647	54	Serial 7 RcvQ full	8664	9664
33	Power up	8648	9648	55	Serial 8 RcvQ full	8665	9665
36	Lost Provisioning	8649	9649	56	Net Guardian DX 1 fail	8666	9666
37	DCP Poller Inactive	8650	9650	57	Net Guardian DX 2 fail	8667	9667
38	LAN not active	8651	9651	58	Net Guardian DX 3 fail	8668	9668
41	Modem not responding	8652	9652	59	GLD 1 fail	8669	9669
42	No Dial tone	8653	9653	60	GLD 2 fail	8670	9670
44	Pager Que Overflow	8654	9654	61	GLD 3 fail	8671	9671
45	Notification failed	8655	9655	62	Channel port timeout	8672	9672
46	Craft RcvQ full	8656	9656	63	Craft port timeout	8673	9673

SNMP Manager Functions

Appendix B

The SNMP Manager allows the user to view alarm status, set date/time, issue controls, and perform a resync. The display and tables below outline the MIB object identifiers. Figure 1 begins with dpsRTU, however, the MIB object identifier tree has several levels above it. The full English name is as follows: `root.iso.org.dod.internet.private.enterprises.dps-Inc.dpsAlarmControl.dpsRTU`. Therefore, dpsRTU's full object identifier is 1.3.6.1.4.1.2682.1.2. Each level beyond dpsRTU adds another object identifying number. For example, the object identifier of the Display portion of the ControlGrid is 1.3.6.1.4.1.2682.1.2.3.3 because the object identifier of dpsRTU is 1.3.6.1.4.1.2682.1.2 + the ControlGrid (.3) + the Display (.3).



Tbl. B1 - _OV_vTraps points.

_OV_vTraps (1.3.6.1.4.1.2682.1.2.0)
PointSet (.20)
PointClr (.21)
sumPSet (.101)
sumPClr (.102)
comFailed (.103)
comRestored (.104)
p0001Set (.10001) through p0064Set (.10064)
p0001Clr (.20001) through p0064Clr (.20064)

Tbl. B4 - ControlGrid points.

ControlGrid (1.3.6.1.4.1.2682.1.2.3)
Port (.1)
Address (.2)
Display (.3)
Point (.4)
Action (.5)

Tbl. B2 - Identity points.

Ident (1.3.6.1.4.1.2682.1.2.1)
Manufacturer (.1)
Model (.2)
Firmware Version (.3)
DateTime (.4)
ResyncReq (.5)*

* Must be set to "1" to perform the resync request.

Tbl. B5 - NVRamSection points.

NVRamSection (1.3.6.1.4.2682.1.2.4.1)
NVsNmbr (.1)
NVsData (.2)
NVsStatus (.3)

Tbl. B3 - DisplayGrid points.

DisplayEntry (1.3.6.1.4.1.2682.1.2.2.1)
Port (.1)
Address (.2)
Display (.3)
DispDesc (.4)*
PntMap (.5)*

* For specific Display and PntMap descriptions see table A1.

Tbl. B6 - AlarmEntry points.

AlarmEntry (1.3.6.4.1.2682.1.2.5.1)
APort (.1)
AAddress (.2)
ADisplay (.3)
APoint (.4)
APntDesc (.5)*
AState (.6)

* For specific point descriptions, see table B7.

Tbl. B7 - Alarm Point Descriptions.

	Description	Port	Address	Display	Points		Description	Port	Address	Display	Points
Display 1	No data*	99	1	1	1-32	Display 11	No data*	99	1	11	1-8
	Undefined**	99	1	1	33-64		Undefined**	99	1	11	9-32
Display 2	No data*	99	1	2	1-32		Power up	99	1	11	33
	Undefined**	99	1	2	33-64		Undefined**	99	1	11	34-35
Display 3	Analog 1	99	1	3	1-4		Lost	99	1	11	36
	Undefined**	99	1	3	5-64		DCP pol inactive	99	1	11	37
Display 4	Analog 2	99	1	4	1-4		LAN not active	99	1	11	38
	Undefined**	99	1	4	5-64		Undefined**	99	1	11	39-40
Display 5	Analog 3	99	1	5	1-4		Modem not	99	1	11	41
	Undefined**	99	1	5	5-64		No dial-tone	99	1	11	42
Display 6	Analog 4	99	1	6	1-4		SNMP trap not	99	1	11	43
	Undefined**	99	1	6	5-64		Pager Que	99	1	11	44
Display 7	Analog 5	99	1	7	1-4		Notification	99	1	11	45
	Undefined**	99	1	7	5-64		Craft RCVQ full	99	1	11	46
Display 8	Analog 6	99	1	8	1-4		Modem RCVQ	99	1	11	47
	Undefined**	99	1	8	5-64		Data 1-8 RCVQ	99	1	11	48-55
Display 9	Analog 7	99	1	9	1-4		NGdx 1-3 fail	99	1	11	56-58
	Undefined**	99	1	9	5-64		GLD 1-3 fail	99	1	11	59-61
Display 10	Analog 8	99	1	10	1-4		CHAN timeout	99	1	11	62
	Undefined**	99	1	10	5-64		CRFT timeout	99	1	11	63

* “No data” indicates that the alarm point is defined but there is no description entered.

** “Undefined” indicates that the alarm point is not used.

ASCII Conversion

Appendix C

The information contained in Table C is a list of ASCII symbols and their meanings. Refer to the bulleted list below to interpret the ASCII data transmitted or received through the data ports. Port transmit and receive activity can be viewed from the Web Browser interface.

- Printable ASCII characters will appear as ASCII.
- Non-printable ASCII characters will appear as labels surrounded by { } brackets (e.g. {NUL}).
- Non-ASCII characters will appear as hexadecimal surrounded by [] brackets (e.g. [IF]).
- A received BREAK will appear as <BRK>.

Tbl. C - ASCII symbols.

Abbreviation	Description	Abbreviation	Description
NUL	Null	DLE	Data Link Escape
SOH	Start of Heading	DC	Device Control
STX	Start of Text	NAK	Negative Acknowledge
ETX	End of Text	SYN	Synchronous Idle
EOT	End of Transmission	ETB	End of Transmission Block
ENQ	Enquiry	CAN	Cancel
ACK	Acknowledge	EM	End of Medium
BEL	Bell	SUB	Substitute
BS	Backspace	ESC	Escape
HT	Horizontal Tabulation	FS	File Separator
LF	Line Feed	GS	Group Separator
VT	Vertical Tabulation	RS	Record Separator
FF	Form Feed	US	Unit Separator
CR	Carriage Return	SP	Space (blank)
SO	Shift Out	DEL	Delete
SI	Shift In	BRK	Break Received

Customer Support

Appendix D

Can't solve that problem? Try visiting our website at www.dpstelecom.com for the latest PDF manual, FAQs, and product discussion forums. The discussion forums are a great place to interact with other users who might have a similar problem.

Frequently Asked Questions

DPS Telecom products are backed by Technical Support representatives who offer you timely, courteous service. If you've tried to work out your problem and need a friendly voice to help you, follow these steps:

Q. *How do I TELNET to DPS devices?*

A. To TELNET into the Net Guardian, connect to Port 2002 (NOT 'Telnet' or any other port options).

Q. *How can I backup what is currently configured and downloaded in my Net Guardian?*

A. Currently the Net Guardian does not support software downloading or configuring. Downloading and configuring are strictly done online to the unit, which is done on a live terminal, (i.e. ProComm or HyperTerminal). We will be coming out with an upgrade soon that will support software configuring. Please be on the lookout for this future update.

Q. *Can I use my Net Guardian as a Proxy Server to activate a serial online menu to my "Third Party" equipment?*

A. Yes. You can use Data ports 1-8 located on the back of the Net Guardian, as long as your equipment's serial port is RS-232 supported. To enable this make sure you use the correct TCP port defined per each Proxy port of the Net Guardian. Establish a Telnet session via the IP address of the Net Guardian and correct TCP port and proceed with connect. Once connected, proceed with your equipment's serial menu commands. Refer the Net Guardian manual for more advanced information on setting up Proxy addressing and Proxy/Data ports 1-8.

Q. *Which version of SNMP is supported by the SNMP agent on the Net Guardian?*

A. SNMP v.1

Q. *How does one configure the Net Guardian to send traps to a manager? Is there a separate SNMP MIB for it? How many managers can the agent send traps to? (Setting the IP address of the manager, the SNMP community string to be used while sending traps...)*

A. The Net Guardian begins sending traps as soon as the managers are defined. The Net Guardian MIB is embedded. The unit supports a global destination trap manager and global communities. Additionally, there are a maximum of eight assignable trap managers (using the notification device / pager table). All managers are designated by their IP addresses.

Q. *Does the Net Guardian support MIB-2 and/or any other standard MIBs?*

A. The Net Guardian supports the bulk of MIB-2.

Q. *Does every SNMP agent running on a Net Guardian box support both the TMon/XM and RTU variables, or will the agent support the TMon/XM variables only with a T/Mon supporting NetGuardian box?*

A. The Net Guardian SNMP agent manages an embedded MIB that supports only the RTU variables. The TMon/XM variables are included in the distributed MIB only to provide a single manager-level MIB for all DPS products.

Q. *The Net Guardian manual talks about 8 relay outputs. How does one control these output ports?*

A. The output relays are controlled by issuing the appropriate set commands against the DPS MIB command grid. The numeric references to the port, address, display and point number associated with the target relay are defined by the RTU and generalized to support multiple-product implementation. The remaining leaf represents the action to be performed and is enumerated to reflect the currently allowed actions.

Q. *What do the terms "alarm point", "display/display number", "port", "address" and "point map" mean within the context of Net*

Guardian operation?

- A. An "alarm point" is the logical term for a single sensed lead the activation of which represents an event that is generally thought to be an alarm condition. There might be a sense lead connected to a low oil probe in a generator or a monitored entry door. A display is a logical group of 64 alarm points and each display has an associated numeric identifier typically called the display number. A port traditionally refers to the physical port over which alarm information is collected using a process generally referred to as polling. In many polling protocols, each polled unit is assigned a unique address. For consistency in information formatting, the port and address concept is often extended to accommodate logical ports and addresses. The Net Guardian reports its internal alarms with a port of 99 and an address of 1. A point map is a single MIB leaf that presents the current status of a 64 alarm point display in an ASCII readable form where a "." represents an alarm point with an inactive sense lead and an "x" represents a point with an active sense lead.
- Q. *How can we associate descriptive information with a "point" for the RTU/granular traps?*
- A. The Net Guardian alarm point descriptions are individually defined using the WEB server interface or the TELNET configuration interface.
- Q. *What characteristics of an alarm point can be configured through software? For instance, can point 4 be used to sense an active-low signal, or point 5 to sense a level or edge?*
- A. The Net Guardian alarm points are level sensed and can be software configured to generate an "alarm" condition on either a high or a low level.
- Q. *How many traps are triggered when a single point is set/cleared? The MIB defines traps like "major alarm set/cleared", "RTU point set" and a lot of granular traps which could imply that more than one trap being sent when a state change occurs on one point.*
- A. Generally, a single state change generates a single trap. One exception to this rule is the first alarm in an "all clear" condition which generates an additional "summary point set" trap. The other exception to this rule is the last alarm that clears going into an "all clear" condition which generates an additional "summary point clear" trap.

Technical Support

DPS Telecom products are backed by Technical Support representatives who offer you timely, courteous service. If you've tried to work out your problem and need a friendly voice to help you, follow these steps:

1. Prepare Relevant Information.

In order to reduce the time it takes to answer your questions, you should have the following information readily available. If you do not have all of this information when you call, our Technical Support representatives can assist you in gathering this information. Please write the information down for easy access:

- User Manual.
- Product Version Number.
- Hardware Serial Number (back right side of unit).
- Computer Information
- IP information for the Net Guardian (IP Address, Subnet, Gateway, etc.)

2. Have access to troubled equipment.

Please be at or near your equipment or computer when you call DPS Technical Support. In that way, we can more efficiently help you when you call.

3. Call during Customer Support hours.

Customer Support hours are Monday through Friday, from 7 a.m. to 6 p.m. Pacific Standard Time. During these hours Technical Support representatives are on duty in our fully-equipped simulation lab. They can simulate your problem and connect to your equipment via modem.

Emergency Assistance: *Emergency assistance is available 24 hours a day, 7 days a week. For emergency assistance after hours, allow the phone to ring until it is answered with a paging message. You will be asked to enter your phone number. An on-call technician will return your call as soon as possible.*

-Numbers-

10BaseT, 7, 43
66 block, 8, 9, 15

-A-

Alarm and Relay connections, 8
Alpha numeric pager, 25
Amphenol connectors, 8-10
Analog Channels, 8, 41
Analog Parameters, 29
ASCII Conversion, 47

-B-

Back Panel Connections, 11
Base Alarms, 35
Base URL, 20, 21
Bell box, 15

-C-

Circuit board, 13
Communication Lines, 7
Component Review, 43
Configuring,
 Analog, 29
 Controls (Relays), 28
 Discrete Alarms, 27
 System Settings, 18
 Logon Password, 19
 Pagers, 24
 Ping Targets, 31
 Port Parameters,
 Ethernet Ports, 20
 Modem Ports, 21
 Craft Ports, 22
 Data Ports, 23
 System Timers, 33
Control Points (Relays), 8
Controls, 28, 36
Craft port, 16, 22, 43
Craft Port Communication Settings, 22
Current draw, 4
Customer Support, 48

-D-

Data Ports, 12, 23, 38
Date and Time, 33

DCPx Net Guardian, 34
Default Gateway, 20
DHCP, 20
Dimensions, 4
Discrete Alarms, 8, 27, 35
Display Mapping, 44
Download Cable, 3

-E-

E-mail paging, 24-25
Echoing, 28
Ethernet, 17-18
Ethernet Ports, 20

-F-

Factory Defaults, 33
Frequently Asked Questions, 48
Functional Diagram, 2
Fuse, 4, 7

-G-

General LCD Display (GLD), 15

-H-

-I-
Interfaces, 4

-J-**-K-****-L-**

LAN, 11, 12, 16-17
LAN Connection, 7
LAN/WAN setup, 17
Latched Controls, 41
LCD Menu, 41
LED Operation, 42
LED bar, 15
Local Connection, 16
Logon Password, 19

-M-

MIB, 21, 45
MIB Installation, 21

Modem, 4, 21, 43
Modem Port Values, 21
Monitoring,
 Analog, 37
 Base Alarms, 35
 Data Port Activity, 38
 Ping Targets, 36
 Proxy Menu, 39
 Relays (Controls), 36
 System Alarms, 37
 System Statistics, 39
Mounting, 4
Mounting Instructions, 6

-N-
Numeric pager, 25

-O-
Operating Temperature, 4
Operating Humidity, 4
Operating Relays, 36

-P-
Pagers setup,
 Alpha numeric, 25
 E-mail, 25
 Numeric, 25
 SNMP, 26
 TCP, 26
 Text, 25
 T/MonXM, 25
Password, 19
PCB Settings, 13, 14
Phone Line Connection, 7, 11
Ping Alarms, 41
Ping Targets, 31, 36
Port Parameters, 20
POTS line, 7
Power Connection, 7
Power Input, 4
PPP Net Guardian, 34
Protocols, 4
Proxy, 12, 40
Proxy Base, 20

-Q-

-R-
Rack ears, 6

Reach-through, 12, 43
Reboot, 41
Relays, 8, 28
Remote Connection (Dial-up), 16

-S-
Saving Changes, 33
Serial ports, 11
SNMP, 18, 20, 24, 26, 27, 28, 31, 44, 45
SNMP Manager Functions, 45
SNMP paging, 26
SNMP Traps, 18, 20, 27, 28, 31, 44
Software Provisioning, 16
Sounds from the Net Guardian 832A, 41
Specifications, 4
Standing Alarms, 41
Subnet Mask, 20
System Alarms, 44
System Settings, 18
System Statistics, 39
System Timers, 32

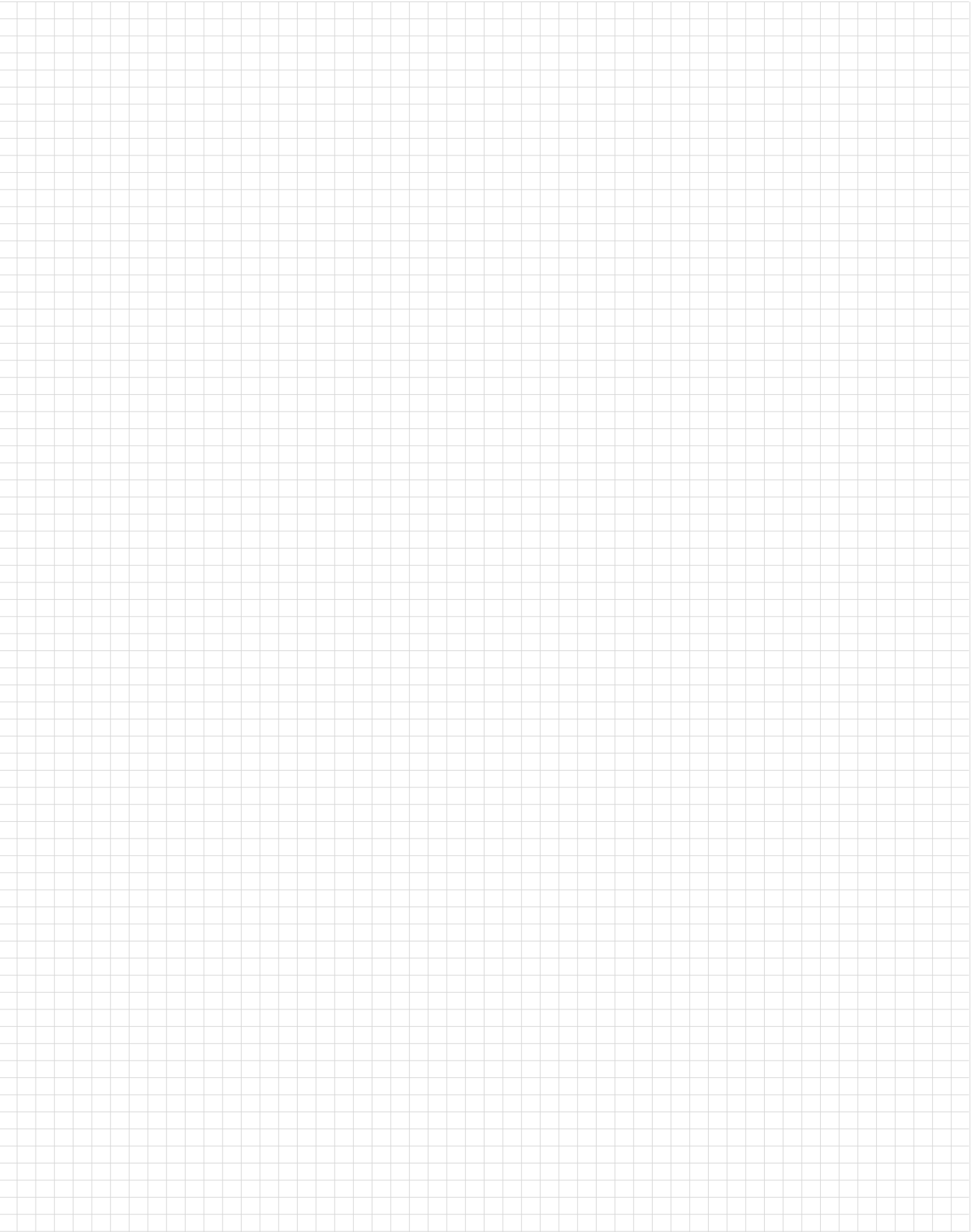
-T-
T/MonXM paging, 25
TCP, 23, 24
TCP paging, 26
Technical Support, 49
TELNET, 7, 12, 16
Text paging, 25
TRAPs, 18, 20, 27, 28, 31, 44

-U-
UDP, 23
Unit Address, 20

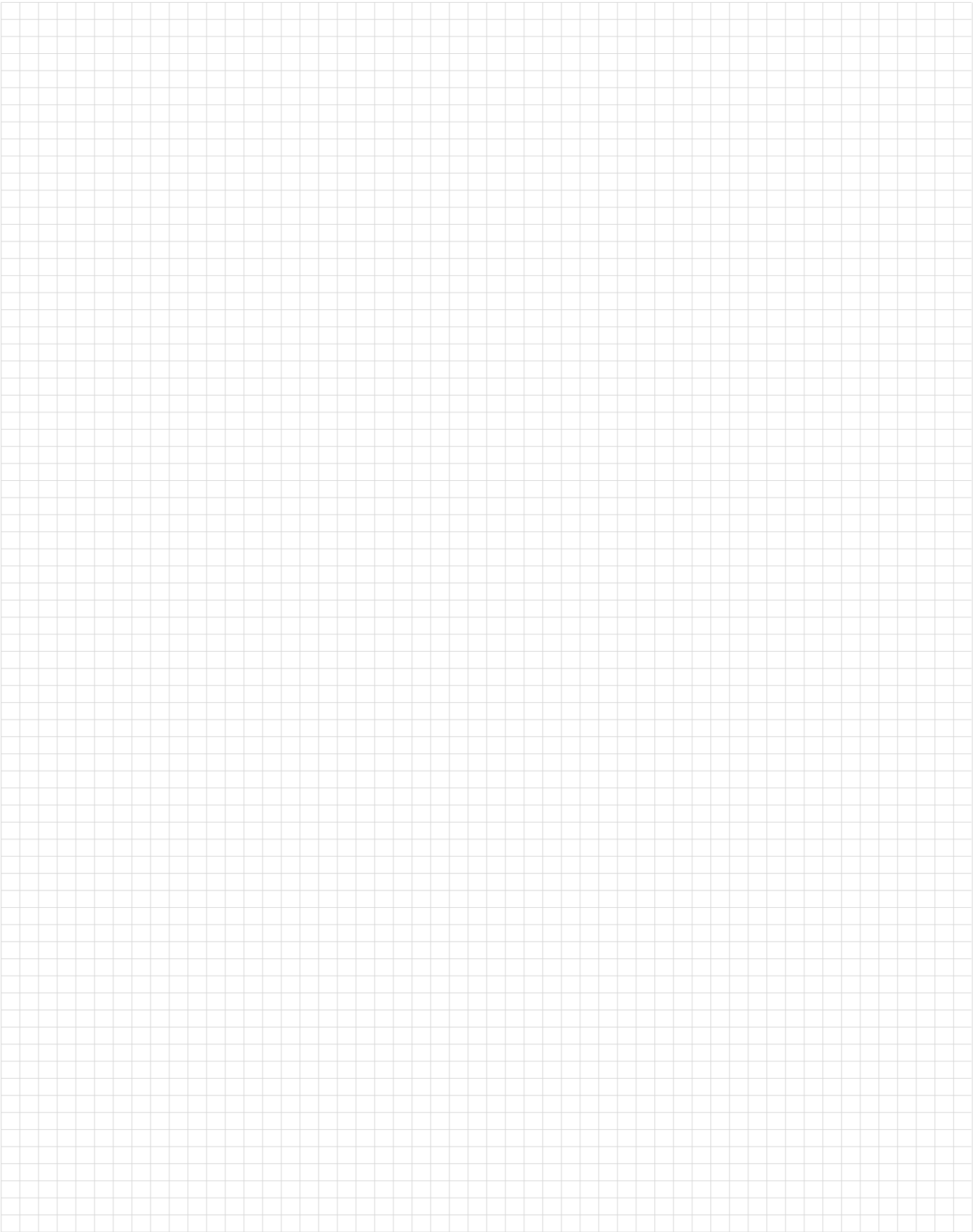
-V-
Viewing Live Target Pings, 39

-W-
Web Server, 16
Web Server Operation Guide, 3, 16
Weight, 4
Wire wrap, 8, 15

-X-
-Y-
-Z-







Warranty

DPS Telecom warrants, to the original purchaser only, that its products a) substantially conform to DPS' published specifications and b) are substantially free from defects in material and workmanship. This warranty expires two years from the date of product delivery with respect to hardware and ninety days from the date of product delivery with respect to software. If the purchaser discovers within these periods a failure of the product to substantially conform to the specifications or that the product is not substantially free from defects in material and workmanship, the purchaser must promptly notify DPS. Within reasonable time after notification, DPS will endeavor to correct any substantial non-conformance with the specifications or substantial defects in material and workmanship, with new or used replacement parts. All warranty service will be performed at the company's office in Fresno, California at no charge to the purchaser, other than the cost of shipping to and from DPS, which shall be the responsibility of the purchaser. If DPS is unable to repair the product to conform to the warranty, DPS will provide at its option one of the following: a replacement product or a refund of the purchase price for the non-conforming product. These remedies are the purchaser's only remedies for breach of warranty. Prior to initial use the purchaser shall have determined the suitability of the product for its intended use. DPS does not warrant a) any product, components or parts not manufactured by DPS, b) defects caused by the purchaser's failure to provide a suitable installation environment for the product, c) damage caused by use of the product for purposes other than those for which it was designed, d) damage caused by disasters such as fire, flood, wind or lightning unless and to the extent that the product specification provides for resistance to a defined disaster, e) damage caused by unauthorized attachments or modifications, f) damage during shipment from the purchaser to DPS, or g) any abuse or misuse by the purchaser.

THE FOREGOING WARRANTIES ARE IN LIEU OF ALL OTHER WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

In no event will DPS be liable for any special, incidental, or consequential damages based on breach of warranty, breach of contract, negligence, strict tort, or any other legal theory. Damages that DPS will not be responsible for include but are not limited to, loss of profits; loss of savings or revenue; loss of use of the product or any associated equipment; cost of capital; cost of any substitute equipment, facilities or services; downtime; claims of third parties including customers; and injury to property.

The purchaser shall fill out the requested information on the Product Warranty Card and mail the card to DPS. This card provides information that helps DPS make product improvements and develop new products.

For an additional fee DPS may, at its option, make available by written agreement only an extended warranty providing an additional period of time for the applicability of the standard warranty.

Technical Support

If a purchaser believes that a product is not operating in substantial conformance with DPS' published specifications or there appear to be defects in material and workmanship, the purchaser should contact our technical support representatives. If the problem cannot be corrected over the telephone and the product and problem are covered by the warranty, the technical support representative will authorize the return of the product for service and provide shipping information. If the product is out of warranty, repair charges will be quoted. All non-warranty repairs receive a 90-day warranty.

“Dependable, Powerful Solutions
that allow users to monitor larger,
more complicated networks with a
smaller, less trained staff”



www.dpstelecom.com
4955 E. Yale Avenue • Fresno, CA 93727
(559) 454-1600 • (800)622-3314 • (559) 454-1688 fax